Jurnal Teknologi

Full Paper

A PERFORMANCE IMPROVED CERTIFICATELESS KEY AGREEMENT SCHEME OVER ELLIPTIC CURVE BASED ALGEBRAIC GROUPS

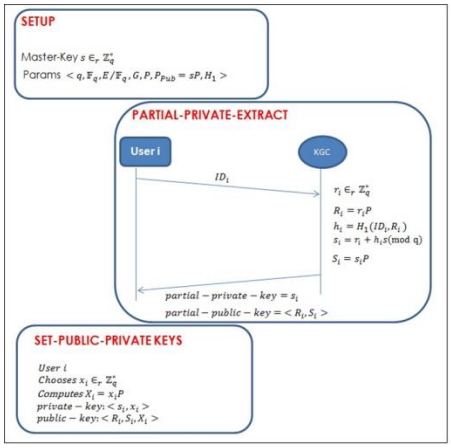
Seyed-Mohsen Ghoreishi*, Ismail Fauzi Isnin, Shukor Abd Razak, Hassan Chizari

Faculty of Computing, Universiti Teknologi Malaysia, 81310 UTM Johor Bahru, Johor, Malaysia

*Corresponding author
mohsen.gh100@gmail.com

Article history
Received
15 May 2015
Received in revised form
1 July 2015
Accepted
11 August 2015

Graphical abstract



Abstract

Due to the importance of key in providing secure communication, various Key Agreement protocols have been proposed in the recent years. The latest generation of Public Key Cryptosystems (PKC) called Certificateless PKC played an important role in the transformation of Key Agreement protocols. In this scientific area, several Key Agreement protocols have been proposed based on Bilinear Pairings. However, pairing operation is known as an expensive cryptographic function. Hence, utilization of pairing operation in the mentioned works made them complex from overall computational cost perspective. In order to decrease the computational cost of Key Agreement protocols, several Certificateless Key Agreement protocols have been proposed by the use of operations over Elliptic Curve based Algebraic Groups instead of using Bilinear Pairings. In this paper, we propose a Pairing-free Certificateless two-party Key Agreement protocol. Our results indicate that our secure protocol is significantly more lightweight than existing related works.

Keywords: Certificateless, key agreement, pairing-free, efficiency

1.0 INTRODUCTION

Due to the inherent problem in Identity-Based cryptosystems named Key Escrow, Al-Riyami *et al*. [1] introduced new type of Public Key Cryptosystem (PKC), named Certificateless PKC. More precisely, in Identity-Based cryptosystems a Trusted Third Party named Private Key Generator (PKG) generates the private key of all users hence there is a possibility of misuse by PKG (e.g. eavesdropping). In order to overcome the mentioned problem, in Certificateless PKC a Trusted Third Party named Key Generation Center (KGC) generates users' partial private-key then each user will generate its own private-key by the use of received partial value from KGC and a chosen random number.

The concept of Certificateless PKC attracted many researchers to propose Certificateless protocols [2-5] including Key Agreement ones. Earlier, most of the proposed Key Agreement protocols in this area were based on Bilinear pairings [6-9]. However, due to the high computational cost performing Pairing operation, various protocols have been proposed based on operations over Elliptic Curve based Algebraic Groups instead of pairings recently [10-17].

In this paper we proposed a Certificateless Key Agreement protocol over Elliptic Curves. The results show that our proposed protocol is significantly lightweight in compare with current Certificateless Pairing-free Key Agreement protocols. Moreover, in the growth of number of established session-key between peer entities, the proposed protocol behaves efficiently.

The rest of this paper is organized as followed. Related works are reviewed in the second section. The third section presents our proposed protocol. The fourth section is dedicated to discussion over performance of

the proposed protocol and related works. The last section concludes this paper.

2.0 RELATED WORKS

A subset of recent Certificateless Key Agreement protocols over Elliptic Curve based algebraic groups are reviewed in this section. The main feature of Pairing-free protocols is that the better performance is gained by eliminating the need to performing expensive computation of Bilinear Pairings.

It is worth to that for more readability we standardized the utilized notations in the considered protocols as followed.

- q: A large prime number
- $\mathbb{F}_q$: A finite field over q
- $E/\mathbb{F}_q$: An elliptic curve over $\mathbb{F}_q$
- G: A subgroup of $E/\mathbb{F}_q$
- P: A generator of the group G
- s: A randomly chosen element of $\mathbb{Z}_q^*$
- P_{Pub}: sP
- H_1, H_2 : Two collision-free one-way hash functions
- ID_i: Identity of user i
- k_s: session key

All considered protocols consist of five main phases which are Setup, Partial-Private Extract, Set-Private-Public Keys, Exchange, and Computation. Since the first three phases are the same in the mentioned works, we just review them once then the rest of the phases will be discussed separately for each protocol.

Figure1 shows Setup, Partial-Private Extract and Set-Private-Public Keys phases of the considered protocols.

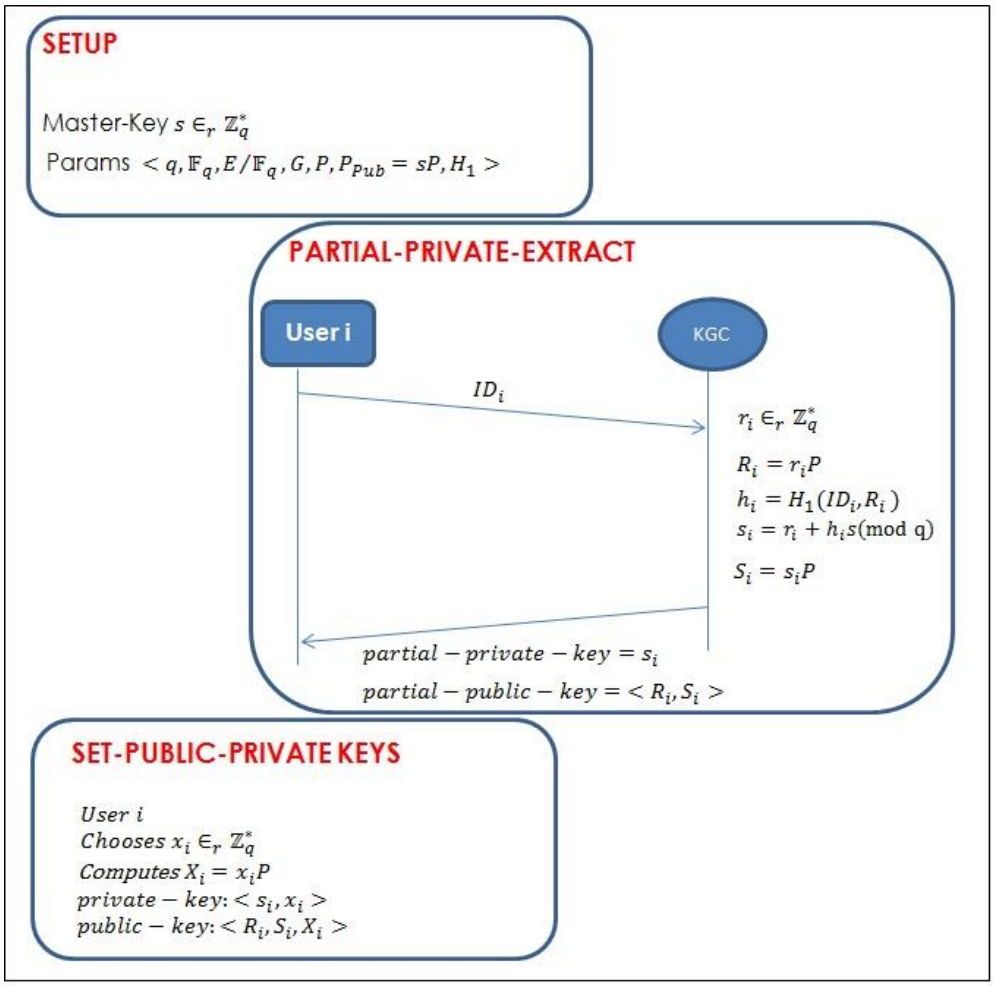


Figure 1 Three first phases of the Certificateless Paring-free Key Agreement protocols

Setup algorithm is responsible to generate Params and Master-Key, after taking the security parameter. It is worth to note that Params is publicly known to all entities whereas the Master-Key is known only by a Trusted Third Party named Key Generation Center (KGC).

The KGC sends a partial-private to a corresponding user whenever a request is made in the Partial-Private

Extract phase. In Set-Private-Public Keys phase, each entity such as i generates its own public and private keys by choosing a random value. Afterward, existing entities can communicate with each other in order to share a session-key in the two last phases.

In continue to what mentioned above, we will demonstrate Exchange and Computation phases of the considered protocols in the rest of this section.

Exchange and Computation phases of proposed protocol by He et al. -2012 [18]

Assume that two entities such as A and B are going to agree on a session key, the proposed protocol by He *et al*. [18] consists of Exchange and Computation phases as followed.

Exchange. In this phase, the following steps are performed by mentioned entities.

(1) Entity A chooses a random $a \in_r \mathbb{Z}_q^*$, and computes the key token $T_A = aP$ then transfer T_A to the entity B.

(2) Entity B chooses a random $b \in_r \mathbb{Z}_q^*$, and computes the key token $T_B = bP$ then transfer T_B to the entity A.

Computation. The considered entities compute the shared secret by performing following computations:

Entity A computes $K_{AB}^1 = (a + s_A)[T_B + S_B]$, $K_{AB}^2 = (a + x_A)[T_B + X_B]$ and $K_{AB}^3 = aT_B$

Entity B computes $K_{BA}^1 = (b + s_B)[T_A + S_A]$, $K_{AB}^2 = (b + x_B)[T_A + X_A]$and $K_{BA}^3 = bT_A$

The computed value in this phase and some public/private values are the inputs for a key driven function that generates the final session key.

Exchange and Computation phases of proposed protocol by Sun et al. -2013 [19]

Assume that two entities such as A and B are going to agree on a session key, the proposed protocol by Sun *et al*. [19] consists of Exchange and Computation phases as followed.

Exchange. In this phase, the following steps are performed by mentioned entities.

(1) Entity A chooses a random $a \in_r \mathbb{Z}_q^*$, and computes the key token $T_A = aP$ then transfer R_A, T_A to the entity B.

(2) Entity B chooses a random $b \in_r \mathbb{Z}_q^*$, and computes the key token $T_B = bP$ then transfer R_B, T_B to the entity A.

Computation. The considered entities compute the shared secret by performing following computations:

Entity A computes $K_{AB}^1 = (a + s_A + x_A)[T_B + S_B + X_B]$, $K_{AB}^2 = (a + 2s_A - x_A)[T_B + 2S_B - X_B]$ and $K_{AB}^3 = (a - s_A - 2x_A)(T_B - S_B + 2X_B)$

Entity B computes $K_{BA}^1 = (b + s_B + x_B)[T_A + S_A + X_A]$, $K_{BA}^2 = (b + 2s_B - x_B)[T_A + 2S_A - X_A]$ and $K_{BA}^3 = (b - s_B - 2x_B)(T_A - S_A + 2X_A)$

The computed value in this phase and some public/private values are the inputs for a key driven function that generates the final session key.

Exchange and Computation phases of proposed protocol by He et al. -2012 [20]

Assume that two entities such as A and B are going to agree on a session key, the proposed protocol by He *et al*. [20] consists of Exchange and Computation phases as followed.

Exchange. In this phase, the following steps are performed by mentioned entities.

(1) Entity A transfers R_A, X_A to the entity B.

(2) Entity B chooses a random $b \in_r \mathbb{Z}_q^*$, and computes the key token $T_B = b(X_A + S_A)$ then transfer R_B, X_B, T_B to the entity A.

(3) Entity A chooses a random $a \in_r \mathbb{Z}_q^*$, and computes the key token $T_A = a(X_B + S_B)$ then transfer T_A to the entity B.

Computation. The considered entities compute the shared secret by performing following computations:

Entity A computes $K_{AB}^1 = (a + s_A)^{-1}T_B + aP$ and $K_{AB}^2 = a(x_A + s_A)^{-1}T_B$

Entity B computes $K_{BA}^1 = (b + s_B)^{-1}T_A + bP$ and $K_{BA}^2 = b(x_B + s_B)^{-1}T_A$

The computed value in this phase and some public/private values are the inputs for a key driven function that generates the final session key.

3.0 THE PROPOSED PROTOCOL

In this paper, we propose an efficient Certificateless Key Agreement protocol that does not require pairings operation. In this section, the proposed protocol is described in detail as followed.

Setup: Setup algorithm is responsible to generate Master-Key $s \in \mathbb{Z}_q^*$ and Params $< q, \mathbb{F}_q, E/\mathbb{F}_q, G, P, P_{Pub}, H_1, H_2 >$, after taking the security parameter. Here, $H_1: \{0,1\}^* \times G \rightarrow \mathbb{Z}_q^*$ and $H_2: \{0,1\}^* \times \{0,1\}^* \times G \times G \rightarrow \mathbb{Z}_q^*$.

Partial-Private-Extract: In this phase, the considered algorithm randomly chooses $r_i \in_r \mathbb{Z}_q^*$, then computes $R_i = r_i P$ and $h_i = H_1(ID_i, R_i)$.The partial-private-key of an entity such as i will be $s_i = r_i + h_i s (\mathrm{mod}\ \mathrm{q})$.

Set-Public-Private Keys: In this phase, each entity such as i randomly chooses $x_i \in_r \mathbb{Z}_q^*$ then computes $P_i = x_i P$. The private and public key of this entity will be $SK_i = (s_i, x_i)$ and $PK_i = (R_i, S_i, P_i)$, respectively. It is worth to note that the value of $S_i = (R_i + h_i P_{pub}) = s_i P$ is publicly computable by all involving entities.

Exchange: In this phase, by considering that two entities such as "A" and "B" are going to agree on a session-key, they act as followed:

(1) A chooses a random $a \in_r \mathbb{Z}_q^*$, computes the key token $T_A = ax_A P_A$ and transfers T_A to the B entity.

(2) B chooses a random $b \in_r \mathbb{Z}_q^*$, computes the key token $T_B = bx_B P_B$ and transfers T_B to the A entity.

Computation: In this phase, the mentioned entities are able to achieve same agreed secret by performing following computations:

A randomly chosen $a \in_r \mathbb{Z}_q^*$, then computes $K_{AB} = (ax_A^2)T_B$
B randomly chosen $b \in_r \mathbb{Z}_q^*$, then computes $K_{BA} = (bx_B^2)T_A$

The computed agreed secret value by two sides in he Computation phase would be the same and it can be proven via following equation.

$$K_{AB} = (ax_A^2)T_B$$
$$= (ax_A^2)bx_BP_B = (ax_A^2)(bx_B^2)P$$
$$= (bx_B^2)(ax_A^2)P = (bx_B^2)ax_AP_A$$
$$= (bx_B^2)T_A$$
$$= K_{BA}$$

The final session-key, k_s, is a key derivation function of K_{AB}:

$$k_s = H_2(ID_A, ID_B, T_A, T_B, K_{AB})$$
$$= H_2(ID_A, ID_B, T_A, T_B, K_{BA})$$

4.0 RESULTS AND DISCUSSION

The main goal of this section is to discuss about the computational cost of the considered protocols (reviewed in the second section) and the proposed one. As mentioned in Introduction, recent Certificateless Key Agreement protocols use operations over elliptic curve based algebraic groups to avoid the high computational cost of performing Pairings operation [21, 22]. To make this issue more clear, Table 1 shows the required time for computation of scalar multiplication over elliptic curve based algebraic groups is around twenty times less than the required time for performing Bilinear Pairing operation [23]. Therefore, the focus of this section is on the related Certificateless two-party Authenticated Key Agreement protocols which are Pairing-free.

Table 1 Required Time for Computation of Two Cryptographic Operations [23]

Operation	Time in milliseconds
Pairing	20.01
ECC-based scalar multiplication	0.83

The computational costs of group operations are shown in Table 2 [24]. Note that in this table the complexity of performing Modular Multiplication is considered as the unit of other operations' complexity.

Table 2 Computational Costs of Group Operations [24]

Notation	Definition and Conversion
T_{MM}	Time complexity for executing the modular multiplication
T_{SM}	Time complexity for executing the elliptic curve scalar multiplication $1T_{SM} \approx 29T_{MM}$
T_{PA}	Time complexity for executing the elliptic curve point addition , $1T_{PA} \approx 0.12T_{MM}$
T_{IN}	Time complexity for executing the modular inversion operation, $1T_{IN} \approx 11.6T_{MM}$

To continue what was mentioned above, we are going to compare the proposed protocol with related protocols reviewed in the second section.

Table 3 gives a comprehensive view over the required computations in Exchange and Computation phases in the proposed protocol and the considered related works.

Table 3 Required computations for the proposed protocol and related works

Authors	Required computations for Exchange and Computation phases from entity A' s viewpoint	Computed Exponentiation (Scalar Multiplication)	Computed point addition
He *et al*. [18]	$T_A = aP$ $K_{AB}^1 = (a + s_A)[T_B + S_B]$ $K_{AB}^2 = (a + x_A)[T_B + X_B]$ $K_{AB}^3 = aT_B$	aP, $(a + s_A)[T_B + S_B]$, $(a + x_A)[T_B + X_B]$, aT_B	$(T_B + S_B), (T_B + X_B)$
Sun *et al*. [19]	$T_A = aP$ $K_{AB}^1 = (a + s_A + x_A)[T_B + S_B + X_B]$ $K_{AB}^2 = (a + 2s_A - x_A)[T_B + 2S_B - X_B]$ $K_{AB}^3 = (a - s_A - 2x_A)(T_B - S_B + 2X_B)$	aP, $(a + s_A + x_A)[T_B + S_B + X_B]$ $(a + 2s_A - x_A)[T_B + 2S_B - X_B]$ $(a - s_A - 2x_A)(T_B - S_B + 2X_B)$	$T_B + S_B + X_B$, $T_B + 2S_B$, $S_B + 2X_B$
He *et al*. [20]	$T_A = a(X_B + S_B)$ $K_{AB}^1 = (a + s_A)^{-1}T_B + aP$ $K_{AB}^2 = a(x_A + s_A)^{-1}T_B$	$a(X_B + S_B)$, $(a + s_A)^{-1}T_B$, aP, $a(x_A + s_A)^{-1}$, $a(x_A + s_A)^{-1}T_B$	$X_B + S_B$ $(a + s_A)^{-1}T_B + aP$
Our proposed Protocol	$T_A = ax_AP_A$ $K_{AB} = (ax_A{}^2)T_B$	$(ax_A{}^2)$P, $(ax_A{}^2)T_B$	-

Table 4 demonstrates the overall computational costs of the proposed protocol in compare with related works based on the given information in Table 2 and Table 3.

Table 4 Performance comparisons over the proposed protocol and related works

Authors	Performance Consideration	Overall computational cost
He *et al*. [18]	4 T_{SM}+2T_{PA}	116.24
Sun *et al*. [19]	4 T_{SM}+4T_{PA}	116.48
He *et al*. [20]	5T_{SM}+2T_{PA}+2T_{IN}	168.44
Our proposed Protocol	2 T_{SM}+T_{MM}	59

It is apparent from Table 4 that the proposed protocol is significantly more lightweight than the existing related works. It is worth to note that for the sake of simplicity in this table the complexity of computation for Modular Multiplication is considered 1to present the overall cost of computations.

5.0 CONCLUSION

Due to the high complexity of performing Pairings operation, pairing-free protocols became an attractive research area in recent years. In the scope of pairing-free Certificateless Key Agreement protocols, several works have been proposed. In this paper, we propose a Certificateless two-party Key Agreement protocol without pairings. The significant feature of the proposed protocol is the low complexity of computations in compare with related works.

References

[1] Al-Riyami, S. S., Paterson, K. G. 2003. Certificateless Public Key Cryptography. C. S. Laih (ed.). Advances in Cryptology C Asiacrypt 2003. Lecture Notes in Computer Science. 452-473.

[2] Zhang, Z., Wong, D. 2006. Certificateless Public-Key Signature: Security Model and Efficient Construction. In: Zhou, J., Yung, M., Bao, F. eds. *Applied Cryptography and Network Security*. Springer, Heidelberg. 293-308.

[3] Li, X., Chen, K., Sun, L. 2005 Certificateless Signature and Proxy Signature Schemes from Bilinear Pairings. *Lithuanian Mathematical Journal.* 45: 76-83.

[4] Liu, J. K., Au, M. H., Susilo, W. 2007. Self-Generated-Certificate Public Key Cryptography and Certificateless Signature/Encryption Scheme in the Standard Model. In: *2007 ACM Symposium on InformAtion, Computer and Communications Security-ASIACCS'07*.

[5] Yum, D. H., Lee, P. J. 2004. Generic Construction of Certificateless Encryption. In: Laganá, A., Gavrilova, M. L., Kumar, V., Mun, Y., Tan, C. J. K., Gervasi, O. eds.

Computational Science and Its Applications–ICCSA 2004. Springer, Heidelberg. 802-811.
[6] Wang, S. Cao, Z. Dong. X. 2006. Certificateless Authenticated Key Agreement Based On The MTI/CO Protocol. *Journal of Information and Computational Science*. 575-581.
[7] Mandt, T., Tan. C. 2008. Certificateless Authenticated Two-Party Key Agreement Protocols. In: *Proceedings of the ASIAN 2006, in: LNCS, vol. 4435.* Springer-Verlag. 37-44.
[8] Shi, Y., Li. J. 2007. Two-party Authenticated Key Agreement In Certificateless Public Key Cryptography. *Wuhan University Journal of Natural Sciences.* 12(1): 71-74.
[9] Lippold, G., Boyd, C., Nieto, J. 2009. Strongly Secure Certificateless Key Agreement. In: *Pairing 2009*. 206-230.
[10] Hou, M. Xu, Q., 2009. A Two-Party Certificateless Authenticated Key Agreement Protocol Without Pairing. In: *2nd IEEE International Conference on Computer Science and Information Technology*. 412-416.
[11] Baek, J., Safavi-Naini, R. and Susilo, W. 2005. Certificateless Public Key Encryption Without Pairing. In *Proceedings of the 8th International Conference on Information Security. Volume 3650 of LNCS.* Springer-Verlag. 134-148, doi: 10.1007/11556992.
[12] Geng, M., Zhang, F. 2009. Provably Secure Certificateless Two-Party Authenticated Key Agreement Protocol Without Pairing. In: *International Conference on Computational Intelligence and Security.* 208-212.
[13] Yang, G., Tan, C. 2011. Strongly Secure Certificateless Key Exchange Without Pairing. In: *6th ACM Symposium on Information, Computer and Communications Security*. 71-79.
[14] Ghoreishi, S. M., Abd Razak, S., Isnin, I. F., Chizari, H. 2014. New Secure Identity-Based and Certificateless Authenticated Key Agreement protocols without Pairings. In *Proceedings of 2014 International Symposium on Biometrics and Security Technologies (ISBAST), Kuala Lumpur, MALAYSIA*. 188-192.
[15] Ghoreishi, S. M., Abd Razak, S., Isnin, I. F., Chizari, H. 2014. A Novel Secure Two-Party Identity-Based Authenticated Key Agreement Protocol Without Bilinear Pairings. In *Proceedings of 4th World Congress on Information and Communication Technologies (WICT), Malacca, MALAYSIA*. 251-258.
[16] Ghoreishi, S. M., Abd Razak, S., Isnin, I. F., Chizari, H. 2014. An Efficient Pairing-free Certificateless Authenticated Two-party Key Agreement protocol over Elliptic Curves. In *Proceedings of 4th World Congress on Information and Communication Technologies (WICT), Malacca, MALAYSIA*. 259-266.
[17] Ghoreishi, S. M., Abd Razak, S., Isnin, I. F., Chizari, H. 2015. Secure and Authenticated Key Agreement Protocol with Minimal Complexity of Operations in the Context of Identity-Based Cryptosystems. In *Proceedings of 2015 International Conference on Computer, Communication, and Control Technology (I4CT), Kuching, Malaysia.*
[18] He, D. Padhye, S. Chen, J. 2012. An Efficient Certificateless Two-Party Authenticated Key Agreement Protocol, *Computers & Mathematics with Applications.* 64(6): 1914-1926.
[19] Sun, H. Wen, Q. Zhang, H. Jin Z., 2013. A Novel Pairing-Free Certificateless Authenticated Key Agreement Protocol With Provable Security. *Frontiers of Computer Science.* Springer.
[20] He, D. Chen, J. Hu, J. 2012. A Pairing-Free Certificateless Authenticated Key Agreement Protocol. *International Journal of Communication Systems*. 25(2): 221-230.
[21] Chen, L. Cheng, Z. Smart, N. P. 2007. Identity-Based Key Agreement Protocols from Pairings. *International Journal of Information Security.* Springer.
[22] Zhang, F., Safavi-Naini, R., Susilo. W., 2004. An Efficient Signature Scheme From Bilinear Pairings And Its Applications. In *Proceedings of PKC 2004*.
[23] Cao, X., Kou, W., Du, X. 2010. A Pairing-Free Identity-Based Authenticated Key Agreement Protocol With Minimal Message Exchanges. *Information Sciences*. 180: 2895-2903.
[24] Islam, S. H., Biswas, G. P. 2012. A Pairing-Free Identity-Based Authenticated Group Key Agreement Protocol For Imbalanced Mobile Networks. *Ann. Telecommun.* 67(11-12): 547-558.