Secure Lightweight Pairing-Based Key-Agreement Cryptosystems: Issues and Challenges

Seyed-Mohsen Ghoreishi and Ismail Fauzi Isnin

***Abstract*—Although a large number of pairing-based key-agreement cryptosystems have been proposed, there are still a lot of drawbacks. One of the most important disadvantages of mentioned cryptographic functions is that there is not a comprehensive system to satisfy both security and efficiency requirements. Moreover, there is not an integrated document to categorize and present possible challenges. Therefore, we paid particular attention to this issue, unlike other surveys in the area of key-agreement cryptosystems. In this paper, we presented a new method to address possible challenges. Actually, we claim that unlike existing documents, this paper determines possible challenges and open problems in the area of lightweight pairing-based key-agreement cryptosystems. We expect that our findings make other researchers able to classify all presented cryptosystems in this area and help them to follow the best way to solve possible problems in the future researches.**

***Index Terms*—Key-agreement, lightweight, pairing-based.**

I. Introduction

Many researches were done in the area of security and cryptography of resource-constrained platforms and their applications, but there are still a lot of open problems. The main reason is that in critical applications, inappropriate solutions could have crucial consequences in dangerous situations. Moreover, since these platforms usually have constrained memory, computational power, communication capacity and battery power, providing security requires lightweight and Power-Saving protocols.

To solve this problem, for many years, symmetric cryptosystems were the basis of these resource-constrained platforms. Although symmetric cryptographic functions could satisfy these challenges as suitable lightweight cryptosystems, but some problems such as not providing non-repudiation services and key distribution problems caused that recent researches tried to make PKC (**P**ublic **K**ey **C**ryptography) usage in mentioned platforms feasible by the use of lightweight public-key cryptosystems.

To achieve this goal, many researches illustrated that the use of ECC-Based (**E**lliptic **C**urve **C**ryptography Based) cryptosystems is the best way to implement lightweight public-key cryptosystems [1]-[3]. The reason of this claim was based on this fact that these cryptosystems consume less resources than traditional ones [4]. Since mentioned ECC-based cryptosystems were usually in turn widely used in pairing maps, many studies were done to propose more efficient bilinear pairings and the use of them in resource-constrained platforms [5]-[12].

Nowadays, due to the researchers' interest to the pairing-based cryptosystems, many evidences offered various kinds of them. Beside of these, in the context of lightweight cryptosystems, some applications like identity-based key-agreement were attracted by many researchers because of the importance of making secure connection in collaborative and distributed applications. The significance of key establishment in making secure connections persuaded us to study in this scientific area and realize all possible challenges appropriate for future researches. The final goal of this research is to help all researchers in this field and make them able to find the best way to develop an extended key-agreement cryptosystem and evaluate it based on desirable parameters. This development can be achieved based on improving the existing schemes, composing some subsets of them, or via transforming some schemes to other group of schemes. To reach this goal, we first presented a history of making some cryptosystems lightweight in section 2. Actually, this section is more than a review on lightweight cryptosystems. If roughly speaking, we could separate lightweight cryptosystems based on the chosen parameter that made them lightweight. In our scenario, we demonstrated a flow of picked up functions that played the main role in making the final cryptosystem suitable in resource-constrained platforms. This method can help future researchers to focus on a special component in both study and development phase of their work. We continued section 2 in a subsection that introduces some researches in the context of lightweight key-agreement schemes. Then in section 3 we outlined possible challenges in the area of pairing-based key-agreement cryptosystems. These challenges can be useful guidelines to categorize related works. Moreover, we claim that they can cover a wide variety of possible problems in the area of pairing-based key-agreement cryptosystems. So, this document can be very useful for all researchers before reviewing related works and can lead them directly in the right way. Finally, we concluded mentioned subjects at the end of this script.

II. A Review on the Sequence of Lightweight Cryptosystems

Nowadays, many researchers have been tried to develop and implement lightweight cryptosystems. The main impressive reason is that resource-constrained platforms cannot afford to spend too much processing time on additional computations [1]. Therefore, it seems that the use of conventional public-key cryptographic functions (e.g. RSA/DSA) is impractical in these platforms, and the security primitives must depend only on symmetric cryptosystems [1].

Manuscript received December 30, 2012; revised March 12, 2013.

The authors are with the University Technology Malaysia (UTM), Skudai 81310, Johor, Malaysia (e-mail: mohsen.gh100@gmail.com, ismailfauzi@utm.my).

Based on this idea, for many years, solutions relied only on symmetric cryptographic functions [2] (e.g., RC5 [13] and Skip-Jack [14]). Although symmetric cryptosystems are more efficient than public-key ones, the cryptography research community still prefer to use public-key cryptosystems.

It is worth mentioning that despite of higher efficiency, symmetric cryptosystems suffer from some drawbacks (such as not providing non-repudiation services and key-distribution problem). Furthermore, using public-key cryptosystems (instead of symmetric ones) simplifies essential security services including key distribution and key management and hence, reduces transmission power due to less overhead [15] , [16]. Thus, many researches tried to solve these resource-constrains by making PKC feasible in resource-constrained platforms. For example, some of the related works are summarized as follow:

1) A new public-key encryption scheme that has significant advantages in terms of computation time and communication overhead [17].
2) A power-saving public-key cryptosystem that reduces the amount of traffic overhead by simplifying the implementation of a special purpose public-key cryptosystem and reducing the amount of transmission power [15].
3) A study that compared the energy cost of two popular Public-Key cryptosystems which are RSA and ECC and indicating ECC's advantages in terms of having smaller key size, less computation and communication cost and fewer amount of data to be transmitted and stored [4].

Motivated by mentioned materials, cryptography research community concluded that ECC consumes considerably less resources than conventional public-key cryptosystems for a given security level [1]-[3]; it means with respect to the limited resources of resource-constrained platforms, the use of ECC can help developers to implement more efficient public-key cryptographic schemes. Therefore, in recent years ECC has achieved great attention from the cryptography research community.

Based on the most of documents, ECC-based public-key cryptosystems are usually based on pairing maps. Miller algorithm [18] is the basis of the most pairing maps. Also in recent years, PBC (Pairing Based Cryptography)is the basis of the most cryptosystems especially in resource-constrained platforms [2]. The first reason is the development of enhanced classes of these platforms (e.g., Imotes [19]). In addition, the second reason can be the entrance of more efficient pairing-based functions (refer to [20]). Therefore, many researches were done in the area of the efficiency of pairings and the use of them in the resource-constrained platforms that some of them are depicted in Table I.

As shown in the Table I, the efficiency of pairing operations has a high potential for future researches.

It is necessary to say that to make PKC deployment more efficient by the use of pairing-based techniques suitable solutions are needed to validate the public-key of the authorized users. This problem can be solved by the use of PKI (Public Key Infrastructure) which is based on public-key certificates. Nevertheless, it is impossible to use PKI in the most of resource-constrained platforms. The major reason is that utilization of PKI, forces users to store, exchange and verify certificates [2] which is not appropriate for resource-constrained nodes. In addition to so-called problem, in this traditional cryptosystems that CA (Certification Authority) is the basis of solving the public-key validity of authorized entities, the need to a valid certificate for CA's public-key leads to a new problem which is PKI complex management. Therefore, identity-based cryptosystems came into the scientific studies to eliminate these problems. Identity-based cryptography was first presented by Adi Shamir [21] in order to eliminate the need to PKI. After that, identity-based cryptography was an open problem for seventeen years, until Boneh and Franklin could represent the first Provably-Secure identity-based encryption scheme in random-oracle model and under BDH (Certification Authority) assumption [22].

TABLE I: SOME RESEARCHES AROUND THE EFFICIENCY OF PAIRING MAPS

References	Final Results
[5],[6]	Making pairing operations more efficient in the term of speed of running.
[7]	Reducing memory usage and improving the efficiency of the tate-pairing in sensor nodes.
[8]	Demonstrating an efficient implementation of tate-pairing by presenting a pairing-based algorithm.
[9],[10]	Introducing an implementation of tate-pairing in lightweight devices.
[11]	Improving various available pairing algorithms through presenting a preliminary result of computing the tate-pairing in wireless platforms, especially in the terms of computational time and memory usage of lightweight platforms.
[1]	Presenting an efficient implementation of ECC on two of the most popular sensor nodes by the use of pairing computations.
[12]	Presenting a fully functional, fast and lightweight pairing-based library for WSNs, instead of creating a benchmark for pairing computations.

TABLE II: SOME REFERENCES THAT USED IDENTITY-BASED CRYPTOSYSTEMS AS A LIGHTWEIGHT SCHEME

References	Final Results
[3]	Showing that IBE (Identity Based Encryption) can be a useful tool for solving key-distribution problem in sensor nodes.
[23]	Introducing a lightweight and secure identity-based private-key refreshing technique.
[24]	Presenting a suitable lightweight IBE method for sensor platforms and providing practical protocols based on proposed scheme.
[25]	Presenting a lightweight and energy-efficient identity-based key management scheme by the use of a special identity-based encryption scheme.
[16]	Introducing a suitable online/offline identity-based signature scheme for sensor environments.

In recent years, both of pairing-based and identity-based cryptosystems play a significant role in wide range of applications. The main reason is that the use of identity-based cryptosystems will have a high potential to be a basis of the most of cryptographic schemes.

Some investigations on lightweight and high performance identity-based cryptosystems are introduced in Table II.

In addition to what mentioned above, in the context of resource-constrained platforms some applications like identity-based non-interactive key-distribution, key-agreement, identity-based-encryption, and short-signature are more interesting for cryptography research community because of their practical nature [2]. In the next subsection, key-agreement and some of the lightweight identity-based GKA (Group Key Agreement) researches are introduced as a main part of the final goal of

this research.

An Overview of Lightweight Pairing-Based Key-Agreement Schemes

TABLE III-A: A SUBSET OF PRESENTED GROUP KEY-AGREEMENT SCHEMES IN THE FIRST CATEGORY

References	Final Goals	Disadvantages
[28]	Presenting an identity-based group key-agreement protocol through using binary-key-tree structure.	Reducing computation time from n to log n.
[29]	Extending Joux's protocol [30] and designing a TGDH-Based protocol by utilizing ternary-key-tree structure instead of binary-key-tree one.	Not providing authentication (like Joux's protocol [30]).
[31]	Presenting an authenticated extension of the Joux's protocol through combining signatures with key-tree structures.	Providing authentication for proposed TGDH tree structure group key-agreement protocol.
[32]	Presenting a provably-secure tree-based protocol in dynamic scenario through using binary-key-tree structure.	Not considering privacy protection.
[33]	Presenting an identity-based key-agreement protocol for dynamic peer groups by the use of binary-key-tree structure	Computationally efficient, but vulnerable against impersonation attack [34]

The second category of pairing-based key-agreement schemes are based on the Burmester and Desmedt (BD) one [35].

TABLE III-B: A SUBSET OF PRESENTED GROUP KEY-AGREEMENT SCHEMES IN THE SECOND CATEGORY

References	Final Goals	Advantages or Disadvantages
[36], [37]	Presenting two separated schemes in two rounds to acquire two identity-based group key-agreement protocols key-agreement protocols.	Not fully authenticated as claimed.
[38],[39]	Presenting a Solution for [36, 37] against colluding attackers by using a synchronous counter.	The cost of the solution is relatively high.
[40]	Presenting a constant-round protocol based on ECC.	Efficient in the terms of communication and computation power, but "ECC certificates" for authentication is needed.

The popularity of collaborative and distributed applications and their need to privacy protection made key-agreement one of the most important research areas. This class of cryptosystems allows several participants to exchange information over an open network so that they can agree on a shared secret-key. Existing pairing-based key-agreement schemes that first presented by Joux [26], can be classified into three categories based on the structure of the group-key construction. The first group with TGDH tree structure is designed based on Kim, Perrig, and Tsudik's work [27].

The last one contains key-agreement cryptosystems that do not have any special structure like [41] in which shi et al. could present a new one-round group key-agreement protocol to reduce the computation cost.

Some of the presented works in the first and the second category are shown in the tables III-A and III-B. To continue, various researches have been done in identity-based group key-agreement scientific area which is suitable for resource-constrained platforms. Some of them are depicted in Table IV. We claim that although a lot of authenticated key-agreement cryptosystems are presented, there are still a lot of untried challenges. Some of the future research topics are introduced in the next section.

TABLE IV: SOME PRESENTED LIGHTWEIGHT IDENTITY-BASED GROUP KEY-AGREEMENT SCHEMES

Presented protocol	Properties	Advantages
A lightweight group key-establishment protocol [42]	Trade-off between the number of message exchanges and additional computations	-Being suitable for energy-constrained nodes with limited communication capabilities - Reducing the number of message exchanges
A three-round identity-based group key-agreement protocol [43]	Anonymous and practicable for WSNs	- Reducing the computation cost for each entity - Preventing transmission of identities of the group members - Providing privacy protection for network nodes -Supporting dynamic membership for group nodes -Creating a Pseudonym from initiator of the protocol
An elegant non-interactive group key-agreement protocol [44]	Non-interactive and hierarchical	-Minimizing the communication complexity -Reducing the number of transmitted bits
A cluster-based group key-agreement protocol [45]	Can be used in variant modes including contributory, non-contributory, unauthenticated or authenticated	-creating a suitable energy balance -having flexible property which can be used in variant modes -using a few lightweight computations

III. FUTURE CHALLENGES AROUND LIGHTWEIGHT KEY-AGREEMENT CRYPTOSYSTEMS

Due to the main goal of this research, this section briefly introduces possible challenging or extending works that can be considered as possible open problems for a novel research. Some findings are as follow:

A. Designing a New Provably-Secure Lightweight Key-Agreement Cryptosystem

The significant attribute of all schemes in this category is that the core part of them which is key-agreement function is more secure than existing ones. In these schemes, the developer tries to solve a special gap based on the security improvement through one of the methods that are mentioned below:

1) Reduction of the security of the novel cryptosystem to a new hard-problem (and claim that selected hard-problem is more powerful than existing one in the compared scheme)
2) Considering stronger security notions (based on the

attacker's abilities, which the cryptosystem should be secure against).

3) Presenting a provably-secure pairing-based key-agreement cryptosystem in the standard model with the similar efficiency to an existing one in the random-oracle model.

B. Improving the Efficiency or the Performance of Existing Key-Agreement Schemes

All proposed schemes in this group usually focus on a special scheme or a subset of them. Presenting an improved scheme, rather than developing a novel one from security viewpoint, can be done through one of the following ways:

1) Enhancing a key-agreement scheme to be appropriate in resource-constrained platforms with regarding to bandwidth, consuming power, number of computations, memory consumptions and so on.
2) Making an existing key-agreement protocol more efficient form functionally viewpoint through eliminating the Trusted-Third-Party (TTP).
3) Transforming some provably-secure pairing-based schemes (such as encryption, digital signature, identification, etc.) to a key-agreement one and taking the advantages of the first group.

C. Comparing Different Key-Agreement Cryptosystems and Analyzing the Efficiency and Functionality of Them

Although we are going to introduce possible challenges to develop a new key-agreement scheme, it is possible that not to present a novel secure cryptosystem or to improve the efficiency of an existing one, but to categorize other schemes and compare them with a new criterion. In addition, researches that are in this group can suggest new benchmarks and introduce the advantages of suggested or selected schemes by the use of them.

D. Attacking on a Known Key-Agreement Scheme or a Group of Them

Another challenge is to attack against a special scheme rather than to develop a novel one. For instance, we can refer to Shim's key-agreement scheme [46] that Sun et al. in [47] could break it.

E. Presenting Real-World Applications and/ or Performing the Suggested Cryptosystem.

Beside of mentioned challenges, future documents can just select a special key-agreement protocol and utilize it as a building block to suggest a new implementation by the use of selected scheme.

F. Doing any Subsets of All Above

It is possible not to focus on one of the mentioned challenges above, but to do some of them together.

IV. Conclusion

Due to the importance of pairing maps in modern cryptosystems, many researchers tried to make them more efficient. In addition, the popularity of key-agreement cryptosystems, motivated many researchers to present a novel lightweight pairing-based key-agreement scheme through improving existing schemes, composing some of them, transforming some schemes to other group of them, or via other methods that are mentioned in this document. To make future researchers able to focus on a special component before reviewing related works and help them to follow the right way, we have presented possible challenges around lightweight pairing-based key-agreement cryptosystems with a new approach.

References

[1] P. Szczechowiak, L. Oliveira, M. Scott, M. Collier, and R. Dahab, "Nano ECC: Testing the limits of Elliptic Curve Cryptography in Sensor Networks," *EWSN, ser. LNCS*, vol. 4913, 2008.

[2] L.B. Oliveira and R. Dahab, "Pairing-based cryptography for sensor networks," presented at IEEE International Symposium on Network Computing and Applications, Cambridge, MA, July 2006.

[3] L. B. Oliveira, R. Dahab, J. Lpez, F. Daguano, and A. A. F. Loureiro, "Identity-based encryption for sensor networks," in *Proc. 5th IEEE International Conf. Pervasive Computing and Communications Workshops*, pp. 290-294, 2007.

[4] C. Tan, H. Wang, S. Zhong, and Q. Li, "Body sensor network security: an identity-based cryptography approach," in *Proc. 1st ACM conf. Wireless Network Security*, pp. 148-153, 2008.

[5] L. B. Oliveira, M. Scott, J. Lpez, and R. Dahab, "Tiny PBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks," in *Proc. 5th International Conf. Networked Sensing Systems*, pp. 173-180, 2008.

[6] M. Shirase, Y. Miyazaki, T. Takagi, D.-G. Han, and D. Choi, "Efficient implementation of pairing based cryptography on a sensor node," *IEICE Trans*. vol. E92-D, no. 5, pp. 909-917, 2009.

[7] X. Xiong, D. S. Wong, and X. Deng, "Tiny Pairing: Computing Tate pairing on sensor nodes with higher speed and less memory," in *Proc. 8th IEEE International Symposium on Network Computing and Applications*, pp. 187-194, 2009.

[8] P. Barreto, H. Kim, B. Lynn, and M. Scott, "Efficient algorithms for pairing-based cryptosystems" in *Proc. CRYPTO Conf. Advances in Cryptology*, pp. 354-368, 2002.

[9] A. Ramachandran, Z. Zhou, and D. Huang, "Computing Cryptographic Algorithms in Portable and Embedded Devices," presented at the IEEE Portable, 2007.

[10] G. Bertoni, L. Chen, P. Fragneto, K. Harrison, and G. Pelosi. (2005). Computing Tate Pairing on Smartcards. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.83.9125&rep=rep1&type=pdf .

[11] Z. Zhou and D. Huang, "Computing Cryptographic Pairing in Sensors," in *Proc. ACM SIGBED Review, Special Issue on the RTSS Forum on Deeply Embedded Real-Time Computing*, vol. 5, no. 1, Jan. 2008.

[12] X. Xiong, D. S. Wong, and X. Deng, "Tiny Pairing: A Fast and Lightweight Pairing-Based Cryptographic Library for Wireless Sensor Networks," in *Proc. IEEE*, 2010.

[13] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: Security protocols for sensor networks," in *Proc. Conf. Wireless Networks*, pp. 521-534, 2002.

[14] C. Karlof, N. Sastry, and D. Wagner, "Tinysec: A link layer security architecture for wireless sensor networks," in *2nd ACM Sens Sys*, pp. 162-175, Nov. 2004.

[15] G. Gaubatz, J.-P. Kaps, E. Oztruk, and B. Sunar, "State of the art in ultra-low power public key cryptography for wireless sensor networks," in *Proc. Per Sec '05, IEEE*, pp. 146-150, 2005.

[16] J. K. Liu, J. Baek, J. Zhou, Y. Yang, and J. W. Wong, " Efficient online/offline identity-based signature for WSN, " in *Proc. IJIS*, pp. 287-296, 2010.

[17] J. Baek, H. Tan, J. Zhou, and J. Wong, "Realizing stateful public key encryption in wireless sensor Network," in *Proc. IFIP-SEC '08*, pp. 95-108, 2008.

[18] V. Miller. (1986). Short programs for functions on curves. Unpublished manuscript. [Online]. Available: http://tcs.uj.edu.pl/~mistar/pdf/Miller1986ShortPrograms.pdf .

[19] R. M. Kling, "Intel mote: An enhanced sensor network node," in *Int'l Workshop on Advanced Sensors, Structural Health Monitoring, and Smart Structures*, pp. 12-17, Nov. 2003.

[20] P. S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scott, "Efficient algorithms for pairing-based cryptosystems," in *Proc. 22nd Annu. CRYPTO Conf. Advances in Cryptology*, London, UK, pp. 354-368, 2002.

[21] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. CRYPTO Conf. Advances in Cryptology*, pp. 47-53, 1984.
[22] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Proc. CRYPTO Conf. Advances in Cryptology*, pp. 213-229, 2001.
[23] S. Balfe, K. Boklan, Z. Klagsbrun, and K. Paterson, "Key Refreshing in Identity-based Cryptography and its Applications in MANETs," presented at the Military Communications conference MILCOM, 2007.
[24] C. C. Tan, H. Wang, S. Zhong, and Q. Li, "IBE-lite: A lightweight identity based cryptography for body sensor networks," in *Proc. IEEE Trans. Inf Technol Biomed*, pp. 926-932, Sep. 2009.
[25] S. Sankaran, M. I. Husain and R. Sridhar, "IDKEYMAN: An Identity-based Key Management Scheme for Wireless Ad Hoc Body Area Network," presented at the Cyber Security Conference, Albany, NY, June, 2009.
[26] A. Joux, "A One Round Protocol for Tripartite Diffie-Hellman," in *Proc. ANTS 4, LNCS 1838*, pp. 385-394, 2000.
[27] Y. Kim, A. Perrig, and G. Tsudik, "Simple and Fault Tolerant Key Agreement for Dynamic Collaborative Groups," in *Proc. ACM Conf. Computer and Communications Security*, pp. 235-244, 2000.
[28] K. C. Reddy and D. Nalla, "Identity Based Authenticated Group Key Agreement Protocol," in *Proc. INDOCRYPT*, vol. LNCS 2551, pp. 215-233, 2002.
[29] S. Lee, Y. Kim, K. Kim, and D.-H. Ryu, "An Efficient Tree-based Group Key Agreement using Bilinear Map," in *Proc. ACNS*, vol. LNCS 2846, pp. 357-371, 2003.
[30] A. Joux, "The Weil and Tate Pairings as building blocks for public key cryptosystems," in *Proc. International Symposium on Algorithm Number Theory*, vol. LNCS 2369, pp. 20-32, 2002.
[31] R. Barua, R. Dutta, and P. Sarkar, "Provably Secure Authenticated Tree Based Group Key Agreement Protocol Using Pairing," in *Proc. ICICS*, vol. LNCS 3269, pp. 92-104, 2004.
[32] R. Dutta and R. Barua, "Dynamic Group Key Agreement in Tree-Based Setting," in *Proc. ACISP*, vol. LNCS 3574, pp. 101-112, 2005.
[33] S.-T. Wu, J.-H. Chiu, and B.-C. Chieu, "Identity-based Key Agreement for Peer Group Communication from Pairings," *IEICE Trans. Fundamentals*, vol. E88-A, no. 10, pp. 2762-2768, October 2005.
[34] D.-L. Vo and K. Kim, "Security Analysis of an ID-based Key Agreement for Peer Group Communication," *IEICE Trans. On Fundamentals*, 2007.
[35] M. Burmester and Y. Desmedt, "A Secure and Efficient Conference Key Distribution System," *EUROCRYPT*, vol. LNCS 950, pp. 275-286, 1994.
[36] K. Y. Choi, J. Y. Hwang, and D. H. Lee, "Efficient ID-based Group Key Agreement with Bilinear Maps," in *Proc. International Workshop on Practice and Theory in Public Key Cryptography (PKC04)*. Springer-Verlag, 2004.
[37] X. Du, Y. Wang, J. Ge, and Y. Wang. (2003). Id-based authenticated two round multi-party key agreement. [Online]. Available: https://eprint.iacr.org/2003/247
[38] F. Zhang and X. Chen. (2003). Attack on Two ID-based Authenticated Group Key Agreement Schemes. *IACR*. [Online]. Available: https://ePrint Archive Report 2003/259.
[39] F. Zhang and X. Chen, "Attack on an ID-based authenticated group key agreement scheme from PKC 2004," *Information Processing Letters*, vol. 91, pp. 191-193, 2004.
[40] L. Zhu, L. Liao, W. Li, and Z. Zhang, "An Authenticated Constant Round Group Key Agreement Protocol Based on Elliptic Curve Cryptography," *International Journal of Computer Science and Network Security*, vol. 6, no. 8B, 2006.
[41] Y. Shi, G. Chen, and J. Li, "ID-Based One Round Authenticated Group Key Agreement Protocol with Bilinear Pairings," presented at the International Conference on Information Technology: Coding and Computing, 2005.
[42] I. Chatzigiannakis, E. Konstantinou, V. Liagkou, and P. Spirakis, "Design, analysis and performance evaluation of group key establishment in wireless sensor networks," in *2nd Workshop on Cryptography for Ad hoc Networks*, Springer-Verlag, 2006.
[43] Z. Wan, K. Ren, W. Lou, and B. Preneel, "Anonymous id-based group key agreement for wireless networks," in *Proc. IEEE WCNC, Network Track*, 2008.
[44] R. Gennaro, S. Halevi, H. Krawczyk, T. Rabin, S. Reidt, and S. D. Wolthusen, "Strongly-Resilient and Non-interactive Hierarchical Key-Agreement in MANETs," in *Proc. ESORICS*, 2008.
[45] E. Konstantinou, "Efficient Cluster-based Group Key Agreement Protocols for Wireless Ad Hoc Networks," *Journal of Networks and Computer Applications*, vol. 34, no. 1, pp. 384-393, 2011.
[46] K. Shim, "Efficient ID-based authenticated key agreement protocol based on the Weil pairing," *IEEE, Electron Lett*, vol. 39, pp. 653- 654, 2003.
[47] H. Sun and B. Hsieh. (2003). Security analysis of Shim's authenticated key agreement protocols from pairings. Cryptology. [Online]. Available: http://ePrint Archive, Report 2003/113.

Seyed-Mohsen Ghoreishi received his B.S. degree in Computer Engineering (Software) from Shahid-Beheshti University, Tehran, Iran, in 2006. He received his M.S. degree in Information Technology Engineering (in the area of Secure Communications) from Iran University of Science and Technology (IUST), Tehran, Iran, in 2009. He is currently a Ph.D. student in computer science (in the area of Cryptography and Information Security) in the Faculty of Computing at University Technology Malaysia (UTM). His research interests are in the areas of Number-Theory, Cryptography, Secure-Protocols, and Information-Security.

Ismail Fauzi Isnin received his B.S. degree in Computer science from University Technology Malaysia (UTM), in 2001. In 2004, he received his M.S. degree in Network Systems Engineering from University of Plymouth, United Kingdom. He received his Ph.D. in Computer Science from University of Plymouth, United Kingdom, in 2011. He is currently a lecturer in the Faculty of Computing at University Technology Malaysia (UTM).