VOL. 11, NO. 10, MAY 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

APPROPRIATE LIGHTWEIGHT CRYPTOSYSTEMS FOR WIRELESS SENSOR NETWORKS

Shabnam Kasra-Kermanshahi, Mazleena Salleh and Hassan Chizari
Faculty of Computing Universiti Teknologi Malaysia Johor, Malaysia
E-Mail: shabnam.kasra@gmail.com

ABSTRACT

The nature of constrained resources of sensor nodes, beside of the inherent vulnerability, led to proposing many lightweight cryptosystems in Wireless Sensor Networks. In this paper, we have traced the use of appropriate cryptosystems for wireless networks and covered different cryptographic protocols of main primitives, which are Encryption, Digital Signature and Key Agreement. Our unique integrated categorization of the proposed lightweight cryptosystems would be useful for those cryptologists who are developing lightweight and applicable schemes for Wireless Sensor Networks.

Keywords: lightweight cryptography, ECC-based cryptography, bilinear pairings, encryption, digital signature, key agreement.

INTRODUCTION

Due to the wide usage of Wireless Sensor Networks (WSNs) many researches were done to design and develop related applications. On one hand, because of the limitation of resources in sensor nodes', proposing lightweight solutions is one of the most significant concerns in such networks. On the other hand, providing security is crucial in open channel communications. Hence, a large variety of lightweight cryptographic schemes have been proposed for Wireless Sensor Networks in order to overcome the problems regarding the constrained memory, computation and communication capacity and battery power.

To solve mentioned problems above, symmetric cryptography was the basis of proposed cryptosystems for many years. The significant prominence of symmetric cryptosystems in compare with Public Key is their higher efficiency especially from computational viewpoint. However, symmetric cryptosystems suffer from a subset of serious problems especially in providing Non-Repudiation and key management services. As a result, many researches have been proposed to make the use of Public Key cryptosystems feasible in Wireless Sensor Networks. Earlier solutions were mostly based on the use of Bilinear Pairings. The role of Bilinear Pairings in making Identity-Based cryptosystems applicable and the significant advantages of Identity-Based cryptography in compare with traditional Public Key ones motivated many researchers of this scientific area to propose lightweight and high performance Identity-Based cryptosystems. It is worth mentioning that in the context of the applications of WSNs, the practical nature of some of them such as Identity-Based non-interactive key-distribution, key-agreement, Identity-Based-encryption and signature make them more interesting [1]. However, Bilinear Pairings are known as expensive cryptographic function. Therefore, the researches in this area were made in two directions; firstly making Pairings operation more efficient (refer to section 5), while recent trends are mostly pairing-free. More precisely, many researchers emphasized on the use of Elliptic Curve Cryptography (ECC) as a practical solution for implementation of lightweight Public Key cryptosystems. Various ECC based cryptosystems have been proposed to prove that they consume fewer resources than traditional Public Key ones. The focus of this paper is on a subset of proposed lightweight Encryption, Digital Signature and Key Agreement schemes, which are appropriate for Wireless Sensor Networks.

The organization of the rest of this paper is as follows. The second section introduces Bilinear Pairings. The history of applicable cryptosystems for Wireless Sensor Networks is provided in Section 3. In Section 4, the importance of ECC in the proposed lightweight cryptosystems is investigated. Section 5 focuses on the role of Bilinear Pairings in the proposed lightweight cryptosystems and probed a subset of researches that have tried to make pairing maps more lightweight than ever before. In Section 6, the position and importance of Identity-Based cryptography is briefly discussed afterward some of the proposed lightweight Identity-Based schemes for Wireless Sensor Networks are investigated. Then three subsequent sections are assigned to three cryptographic primitives; Encryption, Digital Signature and Key Agreement which are appropriate for Wireless Sensor Networks. Finally, the last section presents a summary of the discussions of this literature.

PRELIMINARIES

Because of the importance of Bilinear Pairings in the proposed applicable Identity-based cryptosystems, this section assigns to introducing this mathematical function in more detail.

BILINEAR PAIRING: AN ALGEBRAIC MAP

Bilinear Pairing is a map between two algebraic groups that can satisfy some special properties. Miller algorithm [2] is the basis of the most Bilinear Pairings. To realize the functionality of this category of maps assume that $< G, + >$ and$< G_T, . >$ are two algebraic groups with the same prime order q, and P and Q are two arbitrary elements of the group "G." Based on these assumptions, a

map such as $\hat{e}: G \times G \rightarrow G_T$ can be a bilinear pairing if it can satisfy followed properties:

- Bilinearity: $\forall a, b \in \mathbb{Z}_q^*$, $\hat{e}(aP,bQ) = \hat{e}(P,Q)^{ab}$.
- Non-degeneracy: $\exists P, Q \in G$ that $\hat{e}(P,Q)$ is not equal to the identity element of the group "G_T"
- Computable: $\forall P, Q \in G$, there exists an efficient algorithm to compute $\hat{e}(P,Q)$.

As we will see in Section 5, proposing appropriate lightweight Bilinear Pairings is one of the significant research topics in Wireless Sensor Networks.

APPLICABLE CRYPTOSYSTEMS IN WSNS

These days, Popularity of resource-constrained devices persuaded a large variety of researchers to propose lightweight cryptographic scheme. To reach this goal, replacing conventional public-key cryptosystems such as RSA and DSA by symmetric ones, seems to be one of the possible solutions. For many years, this solution was the basis of proposed lightweight cryptosystems in the resource constrained platforms [1]. A subset of cryptographic algorithms such as RC5 [3] and Skip-Jack [4] are two widely used algorithms to satisfy mentioned drawback.

However, due to some serious disadvantages of symmetric cryptosystems especially in providing non-repudiation services and supporting key-distribution [5], many developers preferred to use public-key cryptosystems. In addition, the use of public-key cryptography can make some essential security services such as key management simpler and leads to reducing the overhead of required transmissions [6, 7].

Mentioned reasons above were sufficient to tempt the researchers to focus on PKC as a solution for limitation of the resources in WSNs. As an example we can refer to the proposed low power public key cryptosystem by Gaubatz *et al.* [6] for the resource-constrained nodes of the Wireless Sensor Networks. In this paper, the authors tried to reduce the traffic overhead by decreasing the amount of transmission power. The other applicable lightweight scheme for the wireless environment is Public Key Encryption protocol proposed by Baek *et al.* [8]. In this scheme, the authors emphasized on the computation time and communication overhead to make the use of proposed Encryption scheme feasible in Wireless Sensor Networks.

THE IMPORTANCE OF ECC BASED SCHEMES IN WSNS

In continue to the mentioned discussions in the previous section, there are several reasons that make Elliptic Curve Cryptography suitable to be used in Public Key cryptosystems for making them more lightweight than ever before. For instance, we can refer to two standard documents; NIST [9] and ECRYPT [10]. As it is illustrated in the Table-1, the use of ECC leads to acquire higher security level but smaller key size in compare with other Public Key cryptosystems, which are defined over the other finite fields.

Table-1. Key size of ECC-based and finite field groups.

Security level (bits) / Category of cryptosystems	80	128	256
ECC-based	160	256	512
Finite Field	1248	3248	15424

a) NIST [9]

Security level (bits / Category of cryptosystems	80	128	256
ECC-based	160	256	512
Finite Field	1024	3072	15360

b) ECRYPT [10]

As a result, ECC received the attention of a large variety of researchers as an appropriate lightweight alternative for symmetric cryptosystems. Mentioned reasons led to proposing several publications which prove that for a given security level, the use of ECC reduces resources' consumption in compare with conventional Public-Key cryptosystems [11, 1, 12]. As another example, we can refer to the study of Tan *et al.* [13] that tried to compare the energy cost of RSA based and ECC based cryptosystems in the environment of Body sensor networks. In this comparison, the authors prove that ECC based cryptosystems consume less computation and communication resources and require fewer amounts of transmitted or stored data with the smaller key size.

PAIRING BASED LIGHTWEIGHT CRYPTOGRAPHIC SCHEMES

In recent years, Bilinear Pairings are the basis of many cryptographic schemes. If roughly speaking, a subset of cryptographic primitive protocols cannot be constructed using other techniques and some others must rely on Bilinear Pairings to improve their functionality [14]. Furthermore, a wide range of lightweight schemes specially those ones which are proposed for resource constrained platforms are based on Bilinear Pairings (for more detail, refer to [1]). It is possible to highlight two reasons of the widely usage of Bilinear Pairings in Wireless Sensor Networks [1]. The first one is developing the enhanced class of some sensor nodes such as Imotes [15], and the other one assigns to the proposing efficient pairing based functions (for more study refer to [16]). The next subsection introduces a subset of proposed lightweight Bilinear Pairings appropriate for the resource constrained nodes in Wireless Sensor Networks.

LIGHTWEIGHT BILINEAR PAIRINGS

As pointed before, Bilinear Pairings have a significant role in the proposed lightweight cryptographic schemes especially in the resource-constrained platforms such as sensor nodes. Since the use of Bilinear Pairings is the basis of a large variety of utilized cryptosystems in WSNs, making a Bilinear Pairing efficient to demonstrate its applicability in Wireless Sensor Networks has been the issue of many proposed literatures. As an example we can refer to what Oliveira *et al.* proposed in [19]. In this paper, the authors proposed an efficient implementation of pairing based cryptographic primitives in sensor nodes. The efficient implementation of pairing proposed by Shirase *et al.* [18] is done over MICAz, which is a widely used sensor node. Xiong *et al.* proposed three algorithms for speeding up the computation and reducing the memory consumption of their intended utilized Bilinear Pairing [19]. Note that they also proposed a programming technique for making the proposed implementation even more lightweight.

The proposed work by Zhou and Huang [19] focused on the feasibility of pairing based protocols in limited computational resources sensor nodes. Moreover, the authors could present a methodology to compute the Tate Pairing on a Supersingular elliptic curve in the MICAz Mote platform [20]. Their different result was based on the fact that without upgrading hardware or optimizing the algorithms and parameters, sensor platforms are not ready to compute expensive Pairing-based cryptographic algorithms.

In contrast to the mentioned result above, Xiong *et al.* in [21] by investigating the performance results of three implemented Pairing-based schemes proved that the use of pairing based cryptosystems is feasible and applicable in WSNs. In this paper, instead of proposing a lightweight Bilinear Pairing, the authors presented a Pairing-based cryptographic fast and lightweight library for WSNs. In addition, by proposing several new algorithms and techniques, they could improve the speed beside of decreasing the memory usage of the mentioned library. Note that, the role of Bilinear Pairings in making Identity-Based cryptosystems applicable had an overlap to proposing lightweight Identity-Based cryptosystems for Wireless Sensor Networks. The next section presents the position and importance of Identity-Based cryptography in Public Key cryptosystems and investigates a subset of proposed lightweight Identity-Based schemes for Wireless Sensor Networks.

IDENTITY-BASED CRYPTOGRAPHIC SCHEMES

As mentioned in Section 3, the use of Public Key cryptography was preferable to Symmetric ones in Wireless Sensor Networks. In order to deploy Public Key cryptography in WSNs, existing entities must be able to validate the public key of other authorized ones. Obviously, the traditional solution is using PKI[1] based on public key certificates. Because of the inherent problem of resource-constrained platforms, the use of PKI is expensive and inapplicable for Wireless Sensor Networks. In addition to the mentioned problem, it is necessary to point out that the use of PKI leads to rely on CA[1] to validate the public key of authorized entities. The result of this solution in turn leads to require a valid certificate for CA's public-key. To understand this problem in more detail, assume that the first entity does not know the CA that certified the second party's public-key. In this scenario, it seems that the first party must verify another certificate. Obviously, if the first party is not able to verify the last certificate, this problem will remain open until she can obtain a verifiable one. As a result, a new problem will occur which is a complex management of PKI environment. To solve mentioned problems, Identity-Based cryptosystems introduced to the cryptographic scientific area. The main contribution of Identity-Based cryptosystems is replacing the users' public-key by an identifier such as telephone number, image, email address or other similar ones. The main goal of the pioneer of Identity-Based cryptography, Adi Shamir, was eliminating the need to Public Key Infrastructures [22].

Nowadays, Identity-Based cryptosystems beside of pairing based ones are the basis of many cryptographic applications. In addition, many researchers have tried to propose lightweight and applicable Identity-Based cryptosystems for Wireless Sensor Networks. A subset of the proposed researches is as followed:

- In [12], the authors claimed that Identity-Based Encryption is Ideal for Wireless Sensor Networks and vice versa.
- In [23], the authors tried to develop a suitable lightweight Identity-Based encryption scheme for resource-constrained sensor platforms in Body Sensor Networks.
- In [24], the authors could present an Identity-Based

key management scheme by the use of Identity-Based Encryption.

- In [7], the authors tried to propose an Identity-Based Digital Signature scheme appropriate for Wireless Sensor Networks.

In continue to the discussions above, it is worth mentioning that in the context of Wireless Sensor Networks, the practical nature of some applications such as Identity-Based non-interactive key-distribution, key-agreement, Identity-Based encryption and digital signature make them more interesting [1]. In continue, we investigated a subset of proposed cryptosystems, which are in the category of Encryption, Digital Signature and Key Agreement appropriate for Wireless Sensor Networks.

APPROPRIATE ENCRYPTION SCHEMES FOR WIRELESS SENSOR NETWORKS

As mentioned in Section 3, limitations of resources in WSNs made traditional Public Key Cryptography a challenging subject (in the area of security issues) in Wireless Sensor Networks. Moreover, Key management problem in the open and unattended environments caused that symmetric encryption become inappropriate in such networks. In addition, symmetric cryptosystems do not provide scalability and non-repudiation [12]. In continue we will introduce two Encryption schemes appropriate for WSNs.

In the [25], Zheng et.al proposed security architecture for WSN named Derivable Public Key (DPK). This scheme utilizes lightweight public key cryptographic algorithm to reduce the total cost. The main contribution of this scheme is to eliminate the need to a Trusted Third Party to distribute and store public keys. It is necessary to point out that the authors claimed that the proposed scheme supports authentication property for both multicast and broadcast communications in WSNs.

Beside of this, the authors of [12] showed that the ideal Encryption scheme for WSNs would be an Identity-Based one. In this paper, the feasibility of implementation of IBE in resource-constrained nodes in WSNs is discussed by testing the results over ATmega128 8-bit AVR processor. In addition, the performance of the implemented scheme was estimated as shown in Table-2.

Table-2. Time estimates of the state pairing (in seconds).

Prime	Coordinate system		
	Projective		Affine
	w/oprecomp.	precomp.	precomp.
Random	13.93s	10.05s	6.37s
Mersenne	9.45s	6.82s	4.33s

The presented results prove that computing the pairing map would be feasible in the determined resource constrained nodes.

APPROPRIATE DIGITAL SIGNATURE SCHEMES FOR WIRELESS SENSOR NETWORKS

In this section we are going to discuss about the Digital Signature scheme suitable for WSNs. In [26], Liu *et al.* proposed an online/offline Identity-Based signature scheme for the Wireless Sensor Network (WSN). The presented Identity-Based scheme does not rely on attached certificates to the signature. This scheme could be implementable in WSNs because of low cost of computational operations and storage. More precisely, it benefits from multi-time usage of offline storage. This property in turn allows the signer to reuse the offline pre-determined information. Furthermore, computations are light due to the use of pairing-free approach in signature generation and verification process. In this paper, a new technique is introduced that made it possible to reuse the offline information. Hence, the signer does not need to execute the offline algorithm for every signing of new messages. In addition, this offline signing algorithm does not rely on secret information provided by the signer. Instead, it is possible to hardcode the offline information into the nodes by manufacturing stage. As a result, it is possible to save communication bandwidth in resource-constrained environment of WSNs. This scheme can be summarized as the following stages.

1- Setup: consider G is a multiplicative group over the prime order q. The PKG[3] selects a random generator $g \in G$ and chooses s $\in_r Z_q^*$. It sets $X = g^x$. Assume that $H: \{0,1\} \rightarrow Z_q^*$is a cryptographic hash function. The public parameters are defined as $params = (G, q, g, X, H)$and the Master-Key is$msk = x$.

2- Extract: The PKG chooses a random $r \in Z_q^*$ to generate a secret key for identity ID, then computes $R \leftarrow g^r \quad s \leftarrow r + H(R, ID)x \bmod q$. The user secret key would be(R, s). The generated secret key must fulfill the equality $g^s = RX^{H(R,ID)}$

3- Offline Sign: The signer should compute $Y\hat{}\, i \leftarrow g2i \; for \; i = 0, \ldots, |q| - 1$.

4- Online Sign: The signer selects $y \in_r Z_q^*$and consider $y[i]$ to be the i-th bit of y. Then define $Y \subset \{1, \ldots, |q|\}$ to be the set of indices such that $y[i] = 1$, computes $\leftarrow \_i \in YY\hat{}\, i - 1 \; h \leftarrow H(Y, R, m) \; z \leftarrow y + h \; s \; mod \; q$. The signature would be (Y, R, z).

5- Verify: To verify the signature $(Y, R, z)$for message m and identity *ID*, the verifier first computes $h \leftarrow H(Y, R, m)$and checks whether$gz = Y\ Rh\ XhH(R, I\ D)$. Then the Verifier accepts the signature if and only if the mentioned equation holds.

The time and energy consumption of this scheme are depicted in Table-3.

Table-3. Time and energy consumption of online/offline Identity-Based signature scheme [26].

Process name	Time (s)	Energy (mJ)
Sign (offline-base station)	**0.293**	**Nill**
Sign (online-MicaZ)	0.896	12.37
Verify (Base station)	0.031	Nill
Verify (MicaZ)	5.61	77.44

APPROPRIATE KEY AGREEMENT SCHEMES FOR WIRELESS SENSOR NETWORKS

Regardless to our discussion over cryptosystem that are compatible with the environment of Wireless Sensor Networks in Section 6, some related Key Agreement schemes will be reviewed in this section. Many researches were done in order to make Identity-Based cryptosystems lightweight and applicable for WSNs. The main contribution in making Key Agreement protocols lightweight is to avoid using Bilinear Pairings [27-33]. The proposed Identity-Based scheme by Cao *et al.* [31] was one the pioneer works in pairing-free Key Agreement area. Beside of inexpensive operation, the proposed protocol has few communication rounds. However, this work could not satisfy security requirement due to what has been discussed in an improved version in [32] proposed by Islam *et al.* in 2012. The former protocol suffers from Known Session Specific Temporary Information Attack and Key Off-Set Attack while the later one has lower cost beside of the providing security. Moreover, the proposed work by Farash *et al.* in [33] is the same as Cao's work from efficiency perspective while it utilized different approach for using Private Key Generator.

CONCLUSIONS

This paper emphasizes on introducing lightweight cryptosystems and their importance in the context of Wireless Sensor Networks. We paid particular attention to ECC based and Pairing-based cryptosystems beside of the lightweight Encryption, Digital Signature, and Key Agreement primitives.

ACKNOWLEDGEMENT

This work is supported by Ministry of Education (MOE), Malaysia and UTM under Vote No. (Q.J130000.2428.02G37).

REFERENCES

[1] L.B. Oliveira and R. Dahab. 2006. "Pairing-based cryptography for sensor networks", In 5th IEEE International Symposium on Network Computing and Applications, Cambridge, MA.

[2] V. Miller. 1986. "Short programs for functions on curves", Unpublished manuscript.

[3] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar. 2002. "SPINS: Security protocols for sensor networks", Wireless Networks, 8(5):521–534. Also appeared in MobiCom'01.

[4] C. Karlof, N. Sastry, and D. Wagner. 2004. "Tinysec: A link layer security architecture for wireless sensor networks", In 2nd ACM SensSys, pages 162–175.

[5] SM. Ghoreishi, IF Isnin. 2013. "Secure lightweight pairing-based key-agreement cryptosystems: Issues and Challenges", IACSIT International Journal of Engineering and Technology, Vol. 5, No. 2.

[6] G. Gaubatz, J.-P. Kaps, E. Oztruk, and B. Sunar. 2005. "State of the art in ultra-low power public key cryptography for wireless sensor networks", In Proc. PerSec '05, pages 146–150. IEEE.

[7] J. K. Liu, J. Baek, J. Zhou, Y. Yang, and J. W. Wong. 2010. "Efficient online/offline identity-based signature for WSN", In IJIS 9(4): 287-296.

[8] J. Baek, H. Tan, J. Zhou, and J. Wong. 2008. "Realizing stateful public key encryption in wireless sensor Network", In Proc. IFIP-SEC '08, pages 95-108. Springer-Verlag.

[9] NIST Recommendation for Key Management Part 1: General, NIST Special publication 800-57.

[10] ECRYPT Yearly Report On Algorithms And Keysizes.

[11] P. Szczechowiak, L. Oliveira, M. Scott, M. Collier, and R. Dahab. 2008. "NanoECC: Testing the limits of Elliptic Curve Cryptography in Sensor Networks," In EWSN 2008, ser. LNCS, vol. 4913. Springer-Verlag.

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

[13] C. Tan, H. Wang, S. Zhong, and Q. Li. 2008. "Body sensor network security: an identity-based cryptography approach", In Proc. 1st ACM conference on Wireless Network Security, pages 148–153. ACM.

[14] R. Dutta, R.Barua, P. Sarkar. 2004. "Pairing-Based Cryptographic Protocols": A Survey.eprint Archive, Report 2004/064.

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

[16] P. S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scott. 2002. "Efficient algorithms for pairing-based cryptosystems", In CRYPTO '02: the 22nd Annual International Cryptology Conference on Advances in Cryptology, pages 354-368, London, UK. Springer-Verlag.

[17] Leonardo B. Oliveira, Diego F. Aranha, Conrado P.L. Gouvêa, Michael Scott, Danilo F. Câmara, Julio López, Ricardo Dahab. 2011. TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks, Computer Communications, Volume 34, Issue 3, 15 March 2011, Pages 485-493.

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

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

[20] Z. Zhou and D. Huang, 2008. "Computing Cryptographic Pairing in Sensors", in Proceeding of ACM SIGBED Review, Special Issue on the RTSS Forum on Deeply Embedded Real-Time Computing, Vol. 5, NO. 1.

[21] X. Xiong, D. S. Wong, and X. Deng, 2010. "TinyPairing: A Fast and Lightweight Pairing-Based Cryptographic Library for Wireless Sensor Networks", In WCNC.

[22] A. Shamir. 1984. "Identity-Based Cryptosystems And Signature Scheme", In Advances In Cryptology-Crypto 1984, Lecture Notes In Comput. Sci. 196, Springer-Verlag, Berlin.

[23] CC Tan, H. Wang, S. Zhong, and Q. Li. 2009. "IBE-lite: A lightweight identity based cryptography for body sensor networks", IEEE Trans Inf. Technol Biomed. 13(6):926 32. Epub 2009 Sep 29.

[24] S. Sankaran, M. I. Husain and R. Sridhar. 2009. "IDKEYMAN: An Identity-based Key Management Scheme for Wireless Ad Hoc Body Area Network", 4th Annual Symposium on Information Assurance, 12th Annual 2009 NYS Cyber Security Conference, Albany, NY.

[25] Zheng, J., Li, J., Lee, M.J. and Anshel, M. 2006. "A lightweight encryption and authentication scheme for wireless sensor networks", Int. J. Security and Networks, Vol. 1, Nos. 3/4, pp.138–146.

[26] Liu, J.K., Baek, J., Zhou, J., Yang, Y., Wong, J.W. 2010. Efficient online/offline identity based signature for wireless sensor network. Cryptology ePrint Archive, Report 2010/003.

[27] SM. Ghoreishi, S. AbdRazak, IF. Isnin, H. Chizari. 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, pp. 188-192.

[28] H. Sun, Q. Wen, H. Zhang, Z. Jin. 2013. A novel pairing-free certificateless authenticated key agreement protocol with provable security, Frontiers of Computer Science, Springer.

[29] SM. Ghoreishi, IF. Isnin, S. AbdRazak, H. Chizari. 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.

[30] SM. Ghoreishi, IF. Isnin, S. AbdRazak, H. Chizari. 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, pp. 251-258.

[31] X. Cao, W. Kou, Y. Yu, R. Sun. 2008. "Identity-based authentication key agreement protocols without bilinear pairings", IEICE Transaction on Fundamentals. E91-A(12):3833-3836.

[32] SK Hafizul Islam, G.P. Biswas. 2012. "An improved pairing-free identity-based authenticated key agreement protocol based on ECC". Procedia Engineering, Volume 30, Pages 499-507, ISSN 1877-7058.

[33] M.S. Farash, M.A. Attari. 2014. "A pairing-free ID-based key agreement protocol with different PKGs". Int. J. Network Security 16(2), 143-148.