Journal of Engineering and Applied Sciences 12 (19): 4809-4813, 2017
ISSN: 1816-949X

A Secure Identity-Based Key Agreement Protocol without Key-Escrow

Seyed-Mohsen Ghoreishi, Ismail Fauzi Isnin, Shukor Abd Razak and Hassan Chizari
Faculty of Computing, Univeristi Teknologi Malaysia (UTM), 81310 Johor, Malaysia

Abstract: In the past decade, pairing-based schemes have been proposed extensively for the cryptographic primitives including key agreement. However, recently researchers have shown an increased interest in Pairing-Free cryptography because of high computational cost of Bilinear Pairings. In this study, we could propose a new two-party pairing-free identity-based authenticated key agreement protocol over elliptic curve based algebraic groups. We could show that beside of supporting security requirements of key agreement protocols, our proposed protocol could overcome to the inherent problem of identity-based cryptosystems named key escrow. In addition, performance of our proposed protocol is improved from complexity of computation perspective in compare with related works.

Key words: Key agreement, identity-based, key escrow, pairing-free, performance, authenticated

INTRODUCTION

In order to establish a shared secret among two or more entities where the channel is considered to be unsecure, a secure key agreement protocol is absolutely indispensable. The main feature of key agreement protocols in the context of identity-based cryptography is that user's public key is driven from their public identity. Identity-based key agreement protocols may vary based on the number of communicating participants and their roles. However, the focus of this study is on two-party key agreement protocols in the context of Identity-Based cryptography.

Identity-Based cryptography has been offered by Shamir (1985) to overcome difficulties of complicated certificate management in traditional Public Key Infrastructures (PKI). The main idea of identity-based cryptography is to consider the user's identity such as e-mail address, digital image, etc., as their public key. Although, this idea seemed to be used widely, it remained unpractical for several years. Finally by Boneh and Franklin (2001) could make this idea applicable. Their work helped to spark a revolution in cryptography and numerous identity-based cryptosystems have been developed followed by their work (such as encryption, digital signature, key agreement and so on). In this way, Bilinear Pairings were the main tool in designing identity-based key agreement protocols (Smart, 2002; Chen and Kudla, 2004; Wang, 2013; Yuan and Li, 2005). Bilinear Pairings which most of them are constructed based on Miller algorithm (Miller, 1986), map two elements of elliptic curve based algebraic groups to a multiplicative group over finite fields (Chen *et al*., 2007).

Although, Bilinear Pairings have been utilized in many cryptosystems, the cost of computing pairing operation is significantly high. In order to make the complexity of computing Bilinear Pairing more understandable we can refer to Table 1 (Ghoreishi and Isnin, 2013).

As shown in this Table 1, the required time of computing ECC-based scalar multiplication is at least twenty times less than performing Bilinear Pairing operation. This reason is enough to persuade researchers to propose pairing-free cryptosystems over elliptic curves.

In this way, recently several researchers struggled to design key agreement protocols without using Bilinear Pairings (Ghoreishi and Isnin, 2013; Ghoreishi *et al*., 2014; Ghoreishi *et al*., 2015a-c; Cao *et al*., 2010; Dutta *et al*., 2004; Zhu *et al*., 2007; Xuefei *et al*., 2008; Islam and Biswas, 2012a, b; Farash and Ahmadia, 2014). In this study, we could propose a lightweight identity-based key agreement protocol that does not require pairing operation.

Preliminaries: This study emphasizes on one of the fundamental components in proving the security of a cryptographic scheme called mathematical hard problem. In fact, the security proof of the considered scheme is given through a reduction to a specified mathematical hard problem. More precisely, the considered adversary

Table 1: Required time for computation of two cryptographic operations (Ghoreishi and Isnin, 2013)

Operation	Time (msec)
Pairing	20.01
ECC-based scalar multiplication	0.83

Corresponding Author: Ismail Fauzi Isnin, Faculty of Computing, Univeristi Teknologi Malaysia (UTM), 81310 Johor, Malaysia

Table 2: Computational costs of group operations

Notations	Definition and conversions
T_{MM}	Time complexity for executing the modular multiplication
T_{SM}	Time complexity for executing the elliptic curve scalar point 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, $1T_{IN} \approx 11.6T_{MM}$

Table 3: Efficiency comparison between our proposed protocol and current related works

Protocols	Xuefei *et al.* (2008)	Islam and Biswas (2012)	Farash and Ahmadia (2014)	SPIIBKA
Efficiency consideration	$5T_{SM}+2T_{PA}$	$5T_{SM}+3T_{PA}$	$5T_{SM}+T_{PA}$	$4T_{SM}+T_{PA}$
Total computational cost	145.24	145.36	145.12	116.12

must solve a well-known hard problem to be able to break the security of the mentioned scheme. There are many well-known mathematical hard problems (Dutta *et al.*, 2004) for more instances) that we just focus on Computational Diffie-Hellman (CDH).

CDH hard problem states that by having a generator (P) of a cyclic group (G) with a prime order (q) and (aP, bP) for randomly chosen values "a" and "b" from the set {0, 1,..., q-1} the desirable output of CDH oracle is the computation of abP.

Literature review: This study assigns to introducing a subset of pairing-free two-party identity-based key agreement protocols. This category of protocols consists of four main algorithms; setup, extraction, exchange and computation. Since, the performance of the related works are investigated in Table 2 and 3, this section just focuses on introducing these protocols, their security analysis and significant contributions. In order to eliminate Bilinear Pairings, Cao *et al.* (2010) could propose an identity-based authenticated key agreement protocol (Cao *et al.*, 2010). The significant contribution of this protocol was reducing the number of message exchanges in compare with previously proposed protocols by Zhu *et al.* (2007). However, Islam and Biswas (2012a, b) could prove that the proposed protocol by Cao is not secure in face with known session specific temporary information and key off-set attacks. Beside of this, mentioned researchers could propose a new protocol to overcome this problem. As another sample of Pairing-Free identity-based key agreement protocols we can refer to the proposed one by Farash and Ahmadia (2014). The significant contribution of mentioned researcher was to consider different private key generators. Performance evaluations of these protocols are represented. The results of study show that our proposed protocol is significantly more efficient than mentioned ones above from computational complexity viewpoint.

MATERIALS AND METHODS

Our proposed protocol: As mentioned earlier in this study we could propose a Secure and Performance Improved Identity-Based Key Agreement protocol (SPIIBKA) which is significantly more efficient than current studies in this scientific area. In this study, we are going to introduce our work in detail.

Phase one setup: The setup algorithm takes the considered security parameter and then outputs master key $s \in_r Z_q^*$ and Params as:

$$<q, F_q, E/F_q, G, P, P_{pub} = sP, H_1, H_2>$$

Where:

q = A large prime number
F_q = A finite field over q
E/F_q = An elliptic curve over F_q
G = A subgroup of E/F_q
P = A generator of the group G

Moreover, it is worth to note that H_1: $\{0, 1\}^* \times G \rightarrow Z_q^*$ and H_2: $\{0, 1\}^* \rightarrow Z_q^*$ are two collision free hash functions. Note that the generated master key is a private value for Private Key Generator (PKG). However, Params are known to all involving entities.

Phase two extraction: Each entity such as i can extract its private key by asking from PKG. PKG operates as:

Randomly chooses $r_i \in_r Z_q^*$,
Computes $R_i = r_i P$
Computes $h_i = H_1 (ID_i, R_i)$
Computes $s_i = r_i + h_i s \pmod q$
Returns $< R_i, s_i >$ as the entity's private key

By considering that two entities such as Alice (A) and Bob (B) want to agree on a session key, they should go through Phase three and Phase four. In our proposed protocol it is assumed that all entities perform a subset of computations and communications before performing the third and fourth phases. Without loss of generality, assume that ID_i is identity of entity I. This entity randomly chooses the value $x_i \in_r Z_q^*$ before computing $X_i = x_i P$, $q_i = s_i + H_2 (ID_i) x_i$ and $Q_i = q_i P$.

Phase three exchange: Based on our proposed protocol, communicating parties who are going to agree on a group of session keys must transmit communicating items before starting the first session. For mentioned entities below,

Alice (A) and Bob (B), communicating items are $<R_A, X_A>$ and $<R_B, X_B>$, respectively. However, the exchange phase consists of following steps:

Algorithm:

Alice:
Chooses a random $t_A \in_r Z^*_q$
Computes $T_A = t_A (s_A + H_2 (ID_A) x_A) P$
Sends T_A, R_A to Bob

Bob:
Chooses a random $t_B \in_r Z^*_q$
Computes $T_B = t_B (s_B + H_2 (ID_B) x_B) P$
Sends T_B, R_B to Alice.

Phase four: computation

In this phase, Alice (A) and Bob (B) can compute the shared secret:
Alice computes $K_{AB} = [t_A (s_A + H_2 (ID_A) x_A)] T_B$
Bob computes $K_{BA} = [t_B (s_B + H_2 (ID_B) x_B)] T_A$
Clearly, the value of K_{AB} and K_{BA} should be the same. Equality of K_{AB} and K_{BA} can be simply proven as below:

$K_{AB} = [t_A (s_A + H_2 (ID_A) x_A)] T_B$
$= [t_A (s_A + H_2 (ID_A) x_A)] [t_B (s_B + H_2 (ID_B) x_B) P]$
$= T_A [t_B (s_B + H_2 (ID_B) x_B) P]$
$= K_{BA}$

Finally, the agreed session key, k_s, is a key derivation function of K_{AB} or K_{BA}.

RESULTS AND DISCUSSION

Security requirements: The main goal of this section is to analyze our proposed scheme from security viewpoint followed by mentioned security requirements by Cheng *et al.* (2005) and Blake *et al.* (1997). Since, the communicating channel is considered unsecure, it is worth to remind that considered adversary is able to reach the values $S_i = s_i P$, X_i and T_i assigned to an entity who possesses ID_i identifier. In the following we will see that our proposed protocol can support introduced security requirements before.

Known-Key Security (KKS): Since, the values of ephemeral secrets, t_A and t_B will be renewed in a new session, the value session-keys of different sessions are unique and independent.

Forward Secrecy (FS): Assume that considered adversary has access private keys of participants, i.e., s_A and S_B. Based on the value of session key $(t_A t_B [(s_A + H_2 (ID_A) x_A)] [(s_B + H_2 (ID_B) x_B)]) P$ adversary is unable to reach the values t_A and t_B as a result computing the session key.

Perfect Forward Secrecy (PFS): Assume that the values of participant's private key and Master-Key, $<s_A, s_B, s>$ had leaked to adversary. Referring to the value of final session key $(t_A t_B [(s_A + H_2 (ID_A) x_A)] [(s_B + H_2 (ID_B) x_B)]) P$ indicates that adversary is unable to reach the values t_A and t_B as a result adversary is unable to compute the value of session key.

Key-Compromise Impersonation (KCI): Here, assume that private key of participant A, s_A had leaked to the adversary. In this condition, adversary must be unable to impersonate B to A. In more detail, considered adversary who knows the value s_A and has transmitted values $T_A = t_A (s_A + H_2 (ID_A) x_A) P$ and $T_B = t_B (s_B + H_2 (ID_B) x_B) P$ must b unable to compute the final session key, $K_{AB} = [t_A (s_A + H_2 (ID_A) x_A)] T_B$. Obviously, computing the session key requires extracting the value t_A from transmitted message $T_A = t_A (s_A + H_2 (ID_A) x_A) P$. To reach this goal, adversary must be able to solve discrete logarithm mathematical hard problem even in a condition that x_A be a known value. As a result our proposed protocol is secure against KCI attack.

Unknown Key-Share Resilience (UKSR): Since, our proposed protocol is secure against KCI, adversary who doesn't have any access to any secret of A and B is unable to impersonate B to A. As a result, it is secure against UKSR attack.

Key Control (KC): Referring to computation phase, indicates that the value of session key $(t_A t_B [(s_A + H_2 (ID_A) x_A)] [(s_B + H_2 (ID_B) x_B)]) P$ depends on both values t_A and t_B. As a result, both participants A and B are involved in generating session keys and cannot predetermine it.

Unknown Session-Specific Temporary Information (USSTI): Assume that the values t_A and t_B are leaked to the adversary. Since considered adversary doesn't have access to the values s_A, s_B, x_A and x_B it is impossible to compute the value of session key which is $(t_A t_B [(s_A + H_2 (ID_A) x_A)] [(s_B + H_2 (ID_B) x_B)]) P$.

Security proof for nonexistence of key-escrow problem: This study is going to show that our proposed protocol is secure against key-escrow problem. Key-escrow is an inherent problem in identity-based schemes. In this category of cryptosystems, PKG generates private key of existing entities. However, this section proves that this inherent drawback doesn't help PKG to compute agreed session key between communicating participants. Following theorem explains this advantage in more detail.

Theorem 1: Assume that A and B are two participants involving in SPIIBKA protocol. The PKG who has access to the Master-Key, s and mentioned participant's private key, s_A and s_B is unable to compute the agreed session key.

Proof: Assume that PKG plays the role of one of the communicating participants. In order to overcome key-escrow problem, PKG must be unable to compute the agreed session key. Without loss of generality, assume that PKG plays the role of participant A. Therefore,

PKG generates t_A and computes $T_A = t_A (s_A+H_2 (ID_A) x_A) P = (t_A s_A) P+H_2 (ID_A) X_A$. In the next step, PKG transmits T_A to B and takes the value $T_B = t_B (s_A+H_2 (ID_B) x_B) P$. In order to takes the value of agreed session key ($t_A t_B [(s_A+H_2 (ID_A) x_A)] [(s_B+H_2 (ID_B) x_B)] P$, PKG must be able to compute the addition of four items in the following equation:

$$K_{AB} = (t_A t_B s_A s_B)P+(t_A t_B s_A H_2 (ID_B)x_B) P+ (t_A t_B s_B H_2 (ID_A)x_A) P+ (t_A t_B H_2 (ID_A)x_A H_2 (ID_B)x_B) P$$

Inability of considered adversary in computing any items of formula above, leads to proving that SPIIBKA protocol doesn't suffer from key-escrow problem. Without loss of generality we choose the last item of equation above ($t_A t_B H_2 (ID_A) x_A H_2 (ID_B) x_B) P$. Here, adversary knows the values t_A, $H_2 (ID_A)$ and $H_2 (ID_B)$. Therefore, mentioned adversary must be able to compute ($t_B x_A x_B$). Although, the value t_B is generated by entity B, we assume that this value had leaked to the adversary. As a result, adversary must be able to compute ($x_A x_B$) P while the values x_A and x_B are not known to him. Since, adversary has access to the values $X_A = x_A P$ and $X_B = x_B P$ while he must be able to compute ($x_A x_B$) P, he will face with CDH problem. Therefore, SPIIBKA protocol is not vulnerable against key-escrow problem.

Because of assuming open channel, PKG knows $T_A = t_A (s_A+H_2 (ID_A) x_A) P$ and $T_B = t_B (s_B+H_2 (ID_B) x_B) P$. In order to compute the value of agreed session key ($t_A t_B [(s_A+H_2 (ID_A) x_A)] [(s_B+H_2 (ID_B) x_B)]) P$, PKG must be able to compute $K_{AB} = [t_A (s_A+H_2 (ID_A) x_A)] T_B$ or $K_{BA} [t_B (s_B+H_2 (ID_B) x_B)] T_A$ Without loss of generality, assume that PKG is going to compute agreed session key through computing $K_{AB} = [t_A (s_A+H_2 (ID_A) x_A)] T_B$.

However, PKG doesn't know the values t_A and x_A. In continue, it is proved that PKG is unable to extract the value t_A. As a result, PKG is unable to compute agreed session key. This result indicates that SPIIBKA doesn't suffer from key-escrow problem.

Because of considering open channel, adversary knows the values R_A and X_A. Since, the values s_A and $H_2 (ID_A)$ are known to PKG, it is possible to compute the value ($t_A P$) after taking T_A from the channel as:

$$t_A P = [T_A - H_2 (ID_A) X_A] s_A^{-1}$$

However, in order to extract the value t_A, the next step is computing t_A from ($t_A P$). Since, there is not any known efficient algorithm to solve discrete logarithm mathematical hard problem, adversary is unable to extract t_A. This fact is sufficient to prove that SPIIBKA doesn't suffer from key-escrow problem.

Performance comparisons: Related to our proposed protocol, several two-party identity-based key agreement protocols without bilinear pairings have been proposed. Xuefei *et al.* (2008) proposed a Pairing-free key agreement protocol that has four scalar multiplications and one point addition. The proposed protocol by Islam and Biswas (2012a, b) has only three scalar multiplications and one point addition. Moreover, in 2014 another pairing-free two-party identity-based key agreement scheme has been proposed by Farash and Ahmadia (2014) that has four scalar multiplications.

Obviously, our proposed pairing-free identity-based key agreement protocol is quite efficient because it just requires three scalar multiplications without any point addition performed by each communicating participant. This claim can be proven via the results by Islam and Biswas (2012a, b) that indicate the complexity of performing algebraic group operations. More precisely, Table 2 represents various computational costs of operations related to algebraic groups. The complexity of executing modular multiplication is considered as a basic unit for the complexity of other operations.

Based on the given information in Table 3 shown the overall computational cost of the considered protocols. Based on what mentioned in Table 3, the proposed protocol, SPIIBKA has lower complexity of computations in compare with current related works.

CONCLUSION

In recent years, there has been an increasing interest in Pairing-free cryptosystems. The key problem regarding to use of Bilinear Pairing is the high computational cost of this operation. In the area of identity-based key agreement protocols several study have been done that could eliminate the need to Bilinear Pairings. In this study, we could propose a secure and authenticated identity-based two-party key agreement protocol without using pairing maps. The results show that beside of supporting security requirements our proposed protocol (SPIIBKA) doesn't suffer from key-escrow drawback. In addition, SPIIBKA is more efficient in compare with existing related works.

ACKNOWLEDGEMENTS

Researchers would like to thank Universiti Teknologi Malaysia and Ministry of Higher Education, Malaysia for sponsoring this research under vote number Q.J13000.2428.01G98. Besides, researchers would like to thank Institut of Sultan Iskandar (ISI) at Universiti Teknologi Malaysia.

REFERENCES

Blake, W.S., D. Johnson and A. Menezes, 1997. Key Agreement Protocols and their Security Analysis. In: Cryptography and Coding, Michael, D. (Ed.). Springer, Berlin, Germany, ISBN:978-3-540-63927-5, pp: 30-45.

Boneh, D. and M. Franklin, 2001. Identity based encryption from the Weil pairing. Proceeding of the Advances in Cryptology-CRYPTO 2001, August 19-23, 2001, California, USA, pp: 213-229.

Cao, X., W. Kou and X. Du, 2010. A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges. Inf. Sci., 180: 2895-2903.

Chen, L. and C. Kudla, 2004. Identity based authenticated key agreement protocols from pairing. Proceedings of the 16th IEEE Computer Security Foundations Workshop, 30 June-2 July, IEEE, pp: 219-233.

Chen, L., Z. Cheng and N.P. Smart, 2007. Identity-based key agreement protocols from pairings. Int. J. Inf. Secur., 6: 213-241.

Cheng, Z., M. Nistazakis, R. Comley and L. Vasiu, 2005. On the indistinguishability-based security model of key agreement protocols-simple cases. IACR. Cryptology E. Pr. Arch., 2005: 129-129.

Dutta, R., R. Barua and P. Sarkar, 2004. Pairing-based cryptographic protocols: A survey. Cryptology ePrint Archive Report 2004/064, 2004. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.3.2043.

Farash, M.S. and A.M. Ahmadia, 2014. A pairing-free id-based key agreement protocol with different pkgs. Int. J. Network Security, 16: 144-149.

Ghoreishi, S.M. and I.F. Isnin, 2013. Secure lightweight pairing-based key-agreement cryptosystems: Issues and Challenges. Int. J. Eng. Technol., 5: 320-320.

Ghoreishi, S.M., I.F. Isnin, S.A. Razak and H. Chizari, 2015a. A Novel Secure Two-Party Identity-Based Authenticated Key Agreement Protocol Without Bilinear Pairings. In: Pattern Analysis, Intelligent Security and the Internet of Things, Ajith, A., K.M. Azah and H.C. Yun (Eds.). Springer, Switzerland, Europe, ISBN:978-3-319-17397-9, pp: 287-294.

Ghoreishi, S.M., I.F. Isnin, S.A. Razak and H. Chizari, 2015b. An Efficient Pairing-Free Certificateless Authenticated Two-Party Key Agreement Protocol Over Elliptic Curves. Proceeding of the Pattern Analysis, Intelligent Security and the Internet of Things, Ajith, A., K.M. Azah and H.C. Yun (Eds.). Springer, Switzerland, Europe, ISBN:978-3-319-17397-9, pp: 295-302.

Ghoreishi, S.M., I.F. Isnin, S.A. Razak and H. Chizari, 2015c. Secure and authenticated key agreement protocol withminimal complexity of operations in the context of identity-based cryptosystems. Proceeding of the 2015 International Conference on Computer, Communications and Control Technology (I4CT), April 21-23, 2015, IEEE, Johor, Malaysia, ISBN:978-1-4799-7953-0, pp: 299-303.

Ghoreishi, S.M., S.A. Razak, I.F. Isnin and H. Chizari, 2014. New secure identity-based and certificateless authenticated Key Agreement protocols without pairings. Proceeding of the 2014 International Symposium on Biometrics and Security Technologies (ISBAST), August 26-27, 2014, IEEE, Johor, Malaysia, ISBN:978-1-4799-6445-1, pp: 188-192.

Islam, S.H. and G.P. Biswas, 2012a. An improved pairing-free identity-based authenticated key agreement protocol based on ECC. Procedia Eng., 30: 499-507.

Islam, S.H. and G.P. Biswas, 2012b. A pairing-free identity-based authenticated group key agreement protocol for imbalanced mobile networks. Ann. Telecommun. Ann. Des Telecommun., 67: 547-558.

Miller, V., 1986. Short programs for functions on curves. Unpublished Manuscript, 97: 101-102.

Shamir, A., 1985. Identity-Based Cryptosystems and Signature Schemes. In: Advances in Cryptology, Blakley, G. and D. Chaum (Eds.). Springer, Berlin, Heidelberg, ISBN: 978-3-540-15658-1, pp: 47-53.

Smart, N.P., 2002. Identity-based authenticated key agreement protocol based on Weil pairing. Electron. Lett., 38: 630-632.

Wang, Y., 2013. Efficient Identity-Based and Authenticated Key Agreement Protocol. In: Transactions on Computational Science, Marina, L.G. and C.J.K. Tan, (Eds.). Springer, Berlin, Germany, ISBN:978-3-642-35839-5, pp: 172-197.

Xuefei, C.A.O., K.O.U. Weidong, Y.U. Yong and S.U.N. Rong, 2008. Identity-based authenticated key agreement protocols without bilinear pairings. IEICE. Trans. Fundam. Electron. Commun. Comput. Sci., 91: 3833-3836.

Yuan, Q. and S. Li, 2005. A new efficient id-based authenticated key agreement protocol. IACR. Cryptology E. Pr. Arch., 2005: 309-309.

Zhu, R.W., G. Yang and D.S. Wong, 2007. An efficient identity-based key exchange protocol with KGS forward secrecy for low-power devices. Theor. Comput. Sci., 378: 198-207.