An Improved Certificateless Public Key Authentication Scheme for Mobile Ad Hoc Networks Over Elliptic Curves

Shabnam Kasra-Kermanshahi and Mazleena Salleh

Abstract Due to the resource constrained property of mobile ad hoc networks (MANETs), making their application more lightweight is one of the challenging issues. In this area, there exists a large variety of cryptographic protocols especially in the context of public key cryptosystems. The difficulty of managing complex public key infrastructures in traditional cryptosystems and the key escrow problem in identity-based ones persuaded many researchers to propose appropriate certificateless cryptosystems for such an environment. In this area, a protocol, named ID-RSA, has been proposed to authenticate the public key in RSA based schemes in the basis of certificateless cryptosystems. Although the security of this protocol is proved, the use of bilinear pairings made it computationally expensive. In this paper, we improved the performance of ID-RSA by the use of elliptic curve based algebraic groups instead of multiplicative ones over finite fields as the output of bilinear pairings. Our results show that our secure protocol is significantly more lightweight than ID-RSA.

Keywords Certificateless PKC · Elliptic curves · Lightweight · MANETs

1 Introduction

The popularity of mobile devices and especial characteristics of mobile ad hoc networks (MANETs) led to various applications from education to military over this type of network. Generally, MANET can be defined as a kind of wireless network, which does not rely on any fixed-infrastructure. In addition, nodes are allowed to join/leave the network at any time; hence, the topology of these

S. Kasra-Kermanshahi (✉) · M. Salleh
Faculty of Computing, Universiti Teknologi Malaysia, Johor Bahru, Johor, Malaysia
e-mail: shabnam.kasra@gmail.com

M. Salleh
e-mail: mazleena@fsksm.utm.my

© Springer International Publishing Switzerland 2015

A. Abraham et al. (eds.), *Pattern Analysis, Intelligent Security and the Internet of Things*, Advances in Intelligent Systems and Computing 355,
DOI 10.1007/978-3-319-17398-6_30

networks is unstable. It should be noted that mentioned features beside the nodes cooperation in running the network functions make MANETs prone to many attacks (e.g. wormhole, blackhole, impersonation, and modification). Since providing security for such environment is a challenging issue, this type of networks became an interesting research area in the recent years [1–3].

In order to provide security for MANETs, two approaches could be considered; attack-oriented and cryptography. Earlier, most of the proposed works were based on the first approach [4–8]. More precisely, the author(s) tried to propose new solutions for possible threats or improve existing works. However, attack-oriented schemes could not resist all types of attacks or combination of them at the same time [1]. The second approach has been used extensively to support security for MANETs in the form of general design framework [1]. In this way, the developers struggled to propose lightweight cryptosystem that could satisfy limitation of resources in MANETs. While the use of symmetric cryptography (SC) is usually acceptable for resource constrained environments [9], the difficulty of key management in SC, persuade developers to apply public key cryptography (PKC) instead [10, 11].

However, traditional PKC could not be the best choice for MANETs because of the need to certificates and public key infrastructure. In 1986, Adi Shamir introduced identity-based cryptography that considered the identity of users as their public key [12]. This idea became practical in 2001 by the illustrious work of Boneh and Franklin [13]. To avoid the inherent problem of identity-based PKC named key escrow, Al-Riyami and Paterson in [14] introduced the concept of certificateless PKC. Afterward, some researchers have been tried to propose schemes based on certificateless PKC in the context of MANETs [15, 16]. Since both of them utilized bilinear pairings which is considered as an expensive cryptographic map, it seems they are not lightweight enough to be used in MANETs. In this paper, we propose a new certificateless scheme that is an enhancement of the proposed scheme in Eissa et al. [15]. More accurately, we could reduce the complexity of computation by the use of elliptic curve based algebraic groups instead of multiplicative ones over finite fields as the output of bilinear pairings.

The rest of this paper is organized as follows. Section 2 explains the required preliminaries. In Sect. 3, ID-RSA protocol has been reviewed. Our proposed scheme is described in Sect. 4 while in Sect. 5, the comparison is presented in the terms of efficiency. Finally, the conclusions are provided in the Sect. 6.

2 Preliminaries

The basis of this section is explaining elliptic curves and their significant role as strong algebraic groups in the cryptography research area. The followed subsection briefly introduces elliptic curves in more detail. Then, a subsection represents the significance of this category of algebraic groups.

2.1 Elliptic Curve Cryptography

Elliptic curves are one of the significant scientific topics in the cryptographic literatures. The significant property of this kind of curves is that a subset of the points over them, beside of a binary operation can generate a beneficial algebraic group.

In the sake of simplicity, it is possible to claim that the elements of mentioned algebraic group are a subset of points of the equation $y^2z = x^3 + axz^2 + bz^3$ with nonzero discriminant ($\Delta = -16[4a^3 + 27b^2]$). Here, a and b are two elements of the determined finite field. Without loss of generality, assume that the coefficients and variables of mentioned equation above are elements of the finite field F_{P^n}. Here, the elements of considered algebraic group are members of the set which is constructed of the points such as (x_0, y_0, z_0). To introduce the elements of this group, it is possible to partition the solutions of mentioned equation into two classes. By assuming the points (0, y_0, 0) as the class of identity element, other ones would be the points of the equation $y^2 = x^3 + ax + b$.

Beside of what explained above, the operation of mentioned algebraic group, named "+", is introduced as following. Without loss of generality, assume that we need to add two points (x_1, y_1) and (x_2, y_2). The final result will be calculated as follows:

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

that $(x_3, y_3) = \left(\lambda^2 - x_1 {-} x_2, \lambda(x_1 - x_3) - y_1\right)$.

The amount of λ is

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, (x_1, y_1) \neq (x_2, y_2) \\ \frac{3x_1^2 + a}{2y_1}, (x_1, y_1) = (x_2, y_2) \end{cases}.$$

Next subsection investigates the advantages of ECC-based algebraic groups that persuaded many researchers to use them.

2.2 Advantages of ECC-based Cryptosystems

In continue to what pointed out in the Sect. 2.1, it is possible to claim that elliptic curves are the basis of a large variety of cryptographic schemes. In compare with RSA-based cryptosystems, the required key size of ECC based is significantly smaller. Tables 1 and 2 represent the suggested key sizes for two mentioned cryptosystems based on the claims of NIST [17] and ECRYPT [18], respectively.

In these tables, the security level refers to the required number of bits of mentioned algebraic group so that the discrete logarithm remains a hard problem.

Table 1 Key sizes of NIST standard [17]

Security level (bits)			
Category of cryptosystems	80	128	256
ECC style	160	256	512
RSA style	1024	3072	15,360

Table 2 Key sizes of ECRYPT standard [18]

Security level (bits)			
Category of cryptosystems	80	128	256
ECC style	160	256	512
RSA style	1248	3248	15,424

3 Review of ID-RSA

In this section, we are going to review the identity-based protocol proposed by Eissa et al. [15]. For the sake of simplicity, we call it ID-RSA. In order to resist RSA cryptanalysis, the authors attempted to ensure that the users' public keys are attainable only by trusted users. Therefore, it is assumed that each user is a part of a coalition. If any user out of one coalition needs public key of a user which is inside the coalition, it should request to the coalition. The detail explanation of this cryptosystem is as followed.

3.1 ID-RSA Phases

It is possible to summarize the ID-RSA in the following main phases.

Setup

The output of this phase is public parameters of the cryptosystem (Params), which are generated by a trusted third party.

$$\text{Params:}\langle G, G_T, q, P, \hat{e}, n, H_1, H_2, H_3 \rangle$$

Here, G is an additive algebraic group as an input of $\hat{e}$:$G \times G \rightarrow G_T$ which is a bilinear pairing that maps elements of mentioned group (such as P) to an element of the multiplicative algebraic group G_T. The order of the mentioned groups is the same at prime number q. In addition, n represents the number of bits of e and N in the RSA cryptosystem. The rest are one-way hash functions that H_1:$\{0,1\}^* \rightarrow G_1^*$, H_2:$G_T \rightarrow \{0,1\}^n$ and H_3:$\{0,1\}^* \rightarrow \{0,1\}^n$.

Node Initialization

In this phase, some of public/private parameters for current users/coalitions will be generated. Three types of public parameters have been considered; identity-key, general-key and public-key. The first one for users/coalitions "i" can be computed by all available users as $Q_i = H_1(ID_i||\text{time})$, whereas the rest are just computable by their owners. More precisely, user/coalition “i” chooses $e_i \in_{\text{random}} \mathbb{Z}_q^*$ then performs RSA key generation algorithm. Similar to RSA, d_i is the private key of the user/coalition “i” and $\langle e_i, N_i \rangle$ represent the corresponding public key. Finally, the mentioned user/coalition computes and publishes its general key $P_i = (d_i \cdot P)$.

Public key obtaining process

In this phase, a user who needs public key of another user inside a coalition can make a request. As a simple scenario, imagine that user A requires public key of user B in the coalition $ID - \text{RSA}_i$, thus by performing the following steps this phase can be done.

Step 1. $A \to ID - \text{RSA}_i{:}P_A, ID_B$

In this step, A sends a request—consist of its general key and identifier B- to $ID - \text{RSA}_i$ coalition. It means, user A needs $\langle e_B, N_B \rangle$.

Step 2. $ID - \text{RSA}_i \to A{:}\langle U, C, W, Y \rangle$

In this step, if A is in the trusted list, the coalition $ID - \text{RSA}_i$ will respond to A tuple $\langle U, C, W, Y \rangle$ that $U = P_i$, $C = e_B \oplus H_2(g_i)$ where g_i is $\hat{e}(Q_A, P_A)^{d_i} \times \hat{e}(d_i Q_i, P_A)$, $W = e_B \cdot P$ and$Y = N_B \oplus H_3(e_B)$.

Step 3. Public key extraction by A

In this step, A can extract $\langle e_B, N_B \rangle$ by a set of computation; $g_A = \hat{e}(d_A Q_A, P_i) \times \hat{e}(Q_i, P_i)^{d_A}$, $e_B = C \oplus H_2(g_A)$, $N_B = Y \oplus H_3(e_B)$ and finally A accepts public key of B if $W = e_B \cdot P$ holds.

ID-RSA correctness

To validate the correctness of ID-RSA, it should be proved that both sides reach the same value through the mentioned computations above. Hence, the value of g_A and g_i should be equal at $\hat{e}(Q_A + Q_i, P)^{d_i d_A}$. It can be proven through the following computations that ID-RSA is a correct scheme.

$$\begin{aligned} g_A &= \hat{e}(d_A Q_A, P_i) \times \hat{e}(Q_i, P_i)^{d_A} \\ &= \hat{e}(Q_A, P)^{d_i d_A} \times \hat{e}(Q_i, P)^{d_i d_A} = \hat{e}(Q_A + Q_i, P)^{d_i d_A} \\ g_i &= \hat{e}(Q_A, P_A)^{d_i} \times \hat{e}(d_i Q_i, P_A) \\ &= \hat{e}(Q_A, P)^{d_i d_A} \times \hat{e}(Q_i, P)^{d_i d_A} = \hat{e}(Q_A + Q_i, P)^{d_i d_A} \end{aligned}$$

4 Proposed Protocol

This section assigns to introducing our proposed certificateless authenticating public key protocol. Similar to ID-RSA, our scheme is constructed based on three phases named setup, node initialization, and public key obtaining process as followed.

Setup

The public output of our scheme, Params, includes following items:

$$\text{Params:}\langle G, q, P, n, H_1, H_2, H_3 \rangle$$

Here, G is a cyclic elliptic curve group with order q and the generator P. The integer number n is the same as n in IDRSA protocol. In addition, $H_1{:}\{0,1\}^* \rightarrow G^*$, $H_2{:}G \rightarrow \{0,1\}^n$ and $H_3{:}\{0,1\}^* \rightarrow \{0,1\}^n$ are three one-way collision-free hash functions.

Node Initialization

Similar to the ID-RSA scheme, the entities can be user or coalition logically. Here, the public and private parameters of mentioned entities are the same as what introduced in ID-RSA. In addition, each entity such as the entity who possesses ID_i generates the parameter $E_i = e_i P_i$.

Public key obtaining process

In this phase, the scenario is similar to what proposed in ID-RSA except that the details of the steps. Here, these steps are as followed:

Step 1. $A \rightarrow \text{Coalition}_i{:}E_A, P_A, ID_B$
In this step, the second input introduces the node A as the entity who sent the request and the third one refers to the identity of the entity who his public key is requested.

Step 2. $\text{Coalition}_i \rightarrow A{:}\langle E_i, U, C, W, Y \rangle$
In this step, the inputs U, C, W and Y are as followed.
$U = P_i$, $C = e_B \oplus H_2(g_i)$ that g_i is equal to $g_i = d_i(E_A + e_i P_A)$ $W = e_B \cdot P$ and $Y = N_B \oplus H_3(e_B)$.

Step 3. In this step, the node A must be able to extract the public key of B (which are e_B and N_B) and verify its authenticity as follows:
First of all, A computes $g_A = d_A(E_i + e_A P_i)$, then computes $e_B = C \oplus H_2(g_A)$. Clearly, the result of g_A and g_i must be the same. In addition, the entity A computes $N_B = Y \oplus H_3(e_B)$. To verify authenticity of the obtained public key, the entity A investigates the equality of ($W = e_B \cdot P$) to decide whether accept or reject the obtained public key of B.

Correctness of the Proposed Protocol

Beside of what mentioned above, it is necessary to prove that the computed values of g_A and g_i are the same. The two equalities below will lead to this result:

$$\begin{aligned} g_A &= d_A(E_i + e_A P_i) = d_A e_i P_i + d_A e_A P_i \\ &= (d_A e_i d_i)P + (d_A e_A d_i)P \\ g_i &= d_i(E_A + e_i P_A) = d_i e_A P_A + d_i e_i P_A \\ &= (d_i e_A d_A)P + (d_i e_i d_A)P \end{aligned}$$

As a result, the functionality of our proposed protocol is logically correct.

Table 3 Computational costs of operations in type 2 and type 3 bilinear pairings [19]

Group operation	Computational cost	
	Type 2	Type 3
Scholar multiplication in G (SM)	1	1
Point addition in G (A)	Negligible	Negligible
Exponent in G_T (E_T)	3	3
Pairing (P)	21	20

5 Efficiency Comparison

The basis of this section is to compare the cost of computing authentication parts of our proposed scheme and ID-RSA, which are the cost of computing g_A and g_i. High expense of computing bilinear pairings [19] is the main reason that made our proposed protocol more efficient than ID-RSA. In order to improve the efficiency of ID-RSA, we have tried to propose our protocol based on group operations of elliptic curves instead of computing bilinear pairings. Table 3 illustrates the cost of operations based on what depicted in [19].

To compare the cost of mentioned two schemes, we have focused on the expense of g_A or g_i parts of "public key obtaining process," as the core of them. Based on the Table 3, the cost of g_A or g_i parts of ID-RSA is equal to "E_T + SM + 2P," while the cost these parts in our proposed scheme is "2(SM) + A," which is quite efficient in compare with ID-RSA.

In the growth of the number of requests for the Step 3 in ID-RSA scheme, the output is more effectual. Based on what is illustrated in Table 3, by assuming that "*n*" is the number of such request, the rate of growth of computational cost for g_A or g_i parts of "public key obtaining process" in our proposed scheme is "2*n*," while this value in IDRSA would be "46*n*" or "44*n*" based on the use of type 2 or type 3 bilinear pairings, respectively.

6 Conclusion

In this paper, we proposed a new certificateless cryptographic protocol to authenticate the public key of other participants. The main contribution of this paper is to improve the computational cost of the ID-RSA protocol by the use of elliptic curve-based algebraic groups instead of multiplicative ones over finite fields as the output of bilinear pairings. Our analysis shows that besides a significant improvement of computational cost, our proposed protocol is much more efficient from the perspective of the rate of computational expense growth in compare with ID-RSA protocol.

References

1. Zhao, S., Akshai, A., Frost, R., Bai, X.: A survey of applications of identity-based cryptography in mobile ad-hoc networks. IEEE Commun. Surv. Tutorials Early Access **14**, 380–400 (2011)
2. Abusalah, L., Khokhar, A., Guizani, M.: A survey of secure mobile ad hoc routing protocols. IEEE Commun. Surv. Tutorials IEEE **10**(4), 78–93 (2008)
3. Sen, C., Salmanian, M., Kellett, M.: A Mobile Ad Hoc Networking Test Bed. DRDC, Defence R&D, Ottawa (2005)
4. Hu, Y., Perrig, A., Johnson,D.: Packet leashes: a defense against wormhole attacks in wireless ad hoc networks. Proceedings of IEEE INFORCOM, 2002
5. Capkun, S., Buttyan, L., Hubaux, J.: Sector: secure tracking of node encounters in multi-hop wireless networks. Proceedings of the ACM workshop on security of ad hoc and sensor networks, 2003
6. Yi, S., Naldurg, P., Kravets, R.: Security-aware ad-hoc routing for wireless networks. Report No. UIUCDCS-R-2002-2290, UIUC, 2002
7. Sanzgiri, K., Dahill, B., Levine, B., Shields, C., Belding-Royer, E.: A secure routing protocol for ad hoc networks. Proceedings of IEEE international conference on network protocols (ICNP), pp. 78–87, 2002
8. Hu, Y., Johnson, D., Perrig, A.: SEAD: secure efficient distance vector routing in mobile wireless ad-hoc networks. Proceedings of the 4th IEEE workshop on mobile computing systems and applications (WMCSA'02), pp. 3–13, 2002
9. Oliveira, L.B., Dahab, R.: Pairing-based cryptography for sensor networks. Presented at IEEE international symposium on network computing and applications, Cambridge, July 2006
10. Gaubatz, G., Kaps, J.-P., Oztruk, E., Sunar, B.: State of the art in ultra-low power public key cryptography for wireless sensor networks. In: Proceedings of Per Sec '05, IEEE, pp. 146–150, 2005
11. Liu, J.K., Baek, J., Zhou, J., Yang, Y., Wong, J.W.: Efficient online/offline identity-based signature for WSN. In: Proceedings of IJIS, pp. 287–296, 2010
12. Shamir, A.: Identity-based cryptosystems and signature schemes. Advances in Cryptology—Crypto. Lecture Notes In Computer Science. Springer, Berlin (1984)
13. Boneh, D., Franklin, M.: Identity based encryption from the weil pairing. Advances in Cryptology—Crypto. Springer, Berlin (2001)
14. Al-Riyami, S.S., Paterson, K.G.: Certificateless public key cryptography. In: Laih, C.S. (ed.) Advances in Cryptology C Asiacrypt. Lecture Notes in Computer Science, pp. 452–473. Springer, Berlin (2003)
15. Eissa, T., Razak, S.A., Ngadi, M.A.: A novel lightweight authentication scheme for mobile ad hoc networks. AJSE **37**, 2179–2192 (2012)
16. Li, L., Wang, Z., Liu, W., Wang, Y.: A certificate less key management scheme in mobile ad hoc networks. 7th international conference on wireless communications, networking and mobile computing, pp 1–4, China, 2011
17. NIST recommendation for key management part 1: general, Nist Special publication 800–57, August 2005
18. ECRYPT yearly report on algorithms and key sizes, 2004
19. Chen, L., Cheng, Z., Smart, N.P.: Identity-based key agreement protocols from pairings. Int. J. Inf. Secur. **6**, 213–241 (2007)