2015 IEEE 2015 International Conference on Computer, Communication, and Control Technology (I4CT 2015), April 21 - 23 in Imperial Kuching Hotel, Kuching, Sarawak, Malaysia

# A Novel Authentication Scheme for Mobile Environments in the Context of Elliptic Curve Cryptography

Shabnam Kasra-Kermanshahi, Mazleena Salleh
Faculty of Computing
Universiti Teknologi Malaysia
Johor, Malaysia
shabnam.kasra@gmail.com , mazleena@fsksm.utm.my

*Abstract*—**The challenge of providing security for Mobile Ad-hoc Networks (MANETs) due to the inherent problems regarding to the use of mobile devices and nonexistence of fixed infrastructures, made them one of the significant topics in security and cryptography research area. In this way, several works have been done to propose lightweight and less energy consuming protocols. However, the use of an expensive cryptographic operation named Bilinear Pairing made the mentioned schemes heavy for such resource constrained environments. In this paper, we could propose an efficient public key authentication scheme over an elliptic curve based algebraic group rather than Bilinear Pairings. The results show that our proposed scheme requires less complex operations in compare with other related ones.**

***Keywords-Certificateless; Authentication; Elliptic Curves; Lightweight; MANETs***

## I. INTRODUCTION

Public Key Cryptography (PKC) is a fundamental branch of science for achieving network and information security [1]. There are three types of PKC as described below.

- Traditional PKC: Certificates are used to ensure about the authenticity of public keys.
- Identity-Based PKC: user's identity is their public key.
- Certificateless PKC: user's public key is generated by both user and Key Generation Center (KGC).

The first type suffers from complexity of certificate management [1] whereas this problem is solved in Identity-Based PKC via the solution given by Shamir [2]. More precisely, in Identity-Based PKC certificates are not required due to the use of user's identity such as email address, digital image, and so on. However, the generation of users' private key by Private Key Generator (PKG) causes another problem for this type of PKC named Key Escrow. It means all information transferred between entities is clear to PKG due to the knowledge of all users' private key. In order to avoid mentioned problem Al-Riyami et al. in [3] suggested Certificateless PKC, a solution that became a beginning of a revolution in PKC. Afterward, various Certificateless PKC have been proposed in different areas in cryptography such Encryption, Digital Signature, Authentication, Key agreement and so on [4-8].

On the other hand, the wide accessibility of mobile devices and wireless networks caused that the applications of mobile environments such as Mobile Ad-hoc Networks (MANETs) are growing rapidly and are not limited to military applications anymore. Due to the fact that these kind of networks do not utilize any fixed infrastructure and to keep the network working, nodes must work cooperatively, security became a challenging issue for such environments. In the beginning, many researches were done to provide solutions to prevent possible attacks such as Blackhole, Wormhole, Impersonation, and Modification [9-14]. However, it is clear that preventing all attacks and any combination of subset of them is not possible in practice [15]. Therefore, Cryptography became more appealing in providing security for the mentioned networks [15]. It might seem that because of the resource limitations in MANETs Symmetric Cryptography would be suitable [16] but it suffers from key management problem. As a result, PKC would be ideal solution [17,18].

As mentioned earlier, Certificateless PKC has been used widely in various areas and MANETs are not exception. In this area several works have been proposed recently [19, 20]. However, the use of an expensive cryptographic operation named Bilinear Pairing made the mentioned schemes heavy for such resource constrained environments. In this paper, we struggled to propose a lightweight public key authentication scheme in the context of Certificateless PKC that utilizes Elliptic Curve Cryptography instead of Pairings. It is worth to note that although our scheme is inspired on the proposed protocol in [19] named IDRSA, due to the elimination of Pairing operation it is much more efficient from complexity of computation perspective.

The rest of this paper is as organized as follows. In the second section required preliminaries have been defined. Section three provides a concise review of the IDRSA protocol. In the fourth section, our proposed scheme is given in details. Section five provides a comparison between our scheme and IDRSA from efficiency viewpoint. At last, the section six presents the conclusion of this paper.

978-1-4799-7958-8/15/$31.00 ©2015 IEEE

## II. PRELIMINARIES

In this section we are going to provide required preliminaries for the rest of this paper. This section consists of two subsections including the utilized notation in the Related works and a brief review of main phases of Certificateless cryptosystems.

### A. Notations

The utilized notations in this paper are described briefly as follows:

- $G$ additive algebraic group
- $G_T$: multiplicative algebraic group
- $q$ : a large prime integer and the order of the mentioned algebraic groups
- $P$: the generator of group $G$
- $s$: master-key
- $\hat{e}: G \times G \rightarrow G_T$ a determined bilinear pairing over mentioned three groups
- $n$ : an integer number that determines the number of bits for the public key of the RSA cryptosystem ($e$ and $N$) for existing entities

### B. Main phases of Certificateless cryptosystems

In this section we present a brief review over main phases of Certificateless cryptosystems that have been introduced by Al-Riyami and Paterson in [3] named Setup, Partial-extraction, Set-secret, Set-private-key, Set-public-key, and the rest is depends on the type of cryptosystem for Encryption it will consists of Encrypt, and Decrypt phases, for Digital Signature it will consists of Sign and Verify and so on.

**Setup:** In this phase by taking security parameter(s), a trusted third party named Key Generator Center (KGC) generates master-key $s \in_r \mathbb{Z}_q^*$ and system parameters (Params).

**Partial- extraction:** The main goal of this phase is generation of a partial-private-key by the use of entities' identifier and the master-key. Therefore, first a one way function of user's identifier is computed. Afterward, the partial-private-key will be generated based on this value and the master-key.

**Set-secret:** In this phase, an entity $i$ who possesses identifier $ID_i$ chooses a random $x_i \in_r \mathbb{Z}_q^*$ as his secret value which will be utilized in the next phase.

**Set-private-key:** By the use of generated secret value in the previous phase and the received partial-private-key in the second phase, each entity can set his private-key in this phase.

**Set-public-key:** In order to generate public-key, in this phase each entity takes Params and the secret value as inputs.

## III. RELATED WORKS

Since, our proposed scheme is inspired on RSA public key authentication scheme proposed by Eissa et al. named IDRSA [20], a brief review over mentioned scheme is provided in this section. The main point about IDRSA is that it can resist RSA cryptanalysis by making users' public keys accessible to only trusted entities. In fact, each user is defined as a member of a coalition and the public obtaining process must be executed in order to obtain the users' public keys from outside of the coalition. The main phases of IDRSA are as below.

***Setup.***

Public parameters of the system (Params) will be generated by a Trust Third Party. The mentioned parameters are as followed:

$$Params: < G, G_T, q, P, \hat{e}, n, H_1, H_2, H_3 >$$

These parameters have been introduced in Preliminaries, and $H_1: \{0,1\}^* \rightarrow {G_1}^*$, $H_2: G_T \rightarrow \{0,1\}^n$, $H_3: \{0,1\}^* \rightarrow \{0,1\}^n$ are one-way hash functions.

***Node Initialization***.

In this phase several public/private parameters for available user/coalitions will be set. In IDRSA, each user/coalition such as "$i$" with identifier $ID_i$ has three public parameters called Identity-key, General-key and Public-key. The first one is computable by all the existing entities $Q_i = H_1(ID_i \parallel time)$ whereas the second one is computable just by its owner $P_i = (d_i.P)$. Finally, the last one is computable only by its owner by accomplishing RSA algorithm hence, $d_i$ is the private-key and $< e_i, N_i >$ will be the public-key.

***Public key obtaining process***.

This process with the following steps should be performed whenever a user (such as A) from outside of the coalition requires public-key of a user inside the coalition (such as$ID - RSA_i$).

**Step1:** $A \rightarrow ID - RSA_i: P_A, ID_B$

User A asks for public-key of user B ($< e_B, N_B >$) from the corresponding coalition while introducing itself.

**Step2:** $ID - RSA_i \rightarrow A: < U, C, W, Y >$

The coalition sends tuple $< U, C, W, Y >$ to A if this user has been mentioned in a trusted list. Here, $U = P_i$, $C = e_B \oplus H_2(g_i)$ that $g_i$ is $\hat{e}(Q_A, P_A)^{d_i} \times \hat{e}(d_i Q_i, P_A)$, $W = e_B.P$ and $Y = N_B \oplus H_3(e_B)$.

**Step3:** Public-key extraction

At this stage user A can gain $< e_B, N_B >$ via following computation; $g_A = \hat{e}(d_A Q_A, P_i) \times \hat{e}(Q_i, P_i)^{d_A}$, $e_B = C \oplus H_2(g_A)$, $N_B = Y \oplus H_3(e_B)$. User A will accepts the public-key if $W = e_B.P$.

It is worth to note that IDRSA can work correctly if and only if the requesting user and the responding coalition reach to the same value. This issue is provable through the equality of $g_A$and $g_i$ at $\hat{e}(Q_A + Q_i, P)^{d_i d_A}$ as shown below.

$$g_A = \hat{e}(d_A Q_A, P_i) \times \hat{e}(Q_i, P_i)^{d_A}$$

$$= \hat{e}(Q_A, P)^{d_i d_A} \times \hat{e}(Q_i, P)^{d_i d_A}$$
$$= \hat{e}(Q_A + Q_i, P)^{d_i d_A}$$

$$g_i = \hat{e}(Q_A, P_A)^{d_i} \times \hat{e}(d_i Q_i, P_A)$$
$$= \hat{e}(Q_A, P)^{d_i d_A} \times \hat{e}(Q_i, P)^{d_i d_A}$$
$$= \hat{e}(Q_A + Q_i, P)^{d_i d_A}$$

Therefore, this scheme works correctly.

## IV. Our Proposed Protocol

In this section we propose our Certificateless public key authentication scheme that does not require any Bilinear Pairings operation. In continue we describe our work in five main phases.

### *1) Setup:*

The Setup phase is an algorithm that must be performed by Key Generation Center (KGC). During this phase, KGC who took security parameters generates confidential master-key $s \in_r \mathbb{Z}_q^*$ and publicly known parameters, Params, as followed:

$$Params: < G, q, P, n, P_{pub} = sP, H_1, H_2, H_3 >$$

It is worth to note that $G$ is a subgroup of an elliptic curve based algebraic group with generator element $P$, the prime number $q$ is the order of mentioned group and the integer $n$ is the same as this item in IDRSA protocol. Moreover, $H_1: \{0,1\}^* \to \mathbb{Z}_q^*$, $H_2: G \to \{0,1\}^n$ and $H_3: \{0,1\}^* \to \{0,1\}^n$ are three collision-free hash functions.

### *2) Partial-extraction:*

As shown in the Figure 1, in Partial-extraction phase, communicating parties, users and coalitions, refer to KGC and obtain the pair of partial public/private keys. Assume that a user or coalition who possesses $ID_i$ identifier contacts with KGC to take corresponding partial public/private keys. KGC randomly chooses $r_i \in_r \mathbb{Z}_q^*$ and computes $R_i = r_i P$, $q_i = H_1(ID_i)$ and $s_i = s + r_i$. Here, $s_i$ is partial private key, while $< R_i, q_i >$ is partial public key. It is necessary to point out that considered user or coalition is able to authenticate the received keys by checking equality $S_i = s_i P = P_{pub} + R_i$.

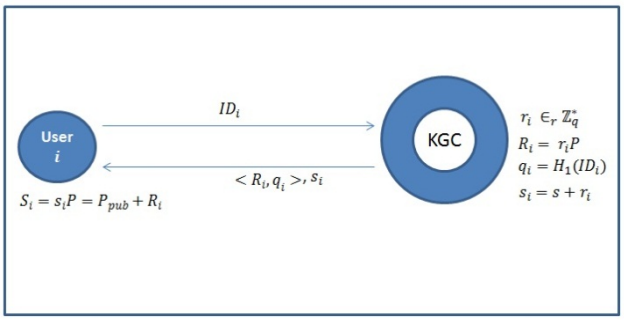


Figure 1. Partial-extraction phase

### *3) Set-secret:*

By performing RSA algorithm, the user or coalition $i$ generates $d_i$ as its secret-value and $< e_i, N_i >$ as the publics (that we call it RSA-public).

### *4) Set-public/private-keys:*

The user or coalition $i$ sets tuple $< R_i, q_i, P_i, < e_i, N_i >>$ as its public-key and the tuple $< s_i, d_i >$ as the corresponding private-key. It is worth to note that here $P_i = d_i P$.

### *5) Public key obtaining process:*

This process with the following steps should be performed whenever a user (such as A) from outside of the coalition requires public-key of a user inside the coalition (such as $Coalition_i$). Figure2 illustrates this process briefly.

- **Step1**: In this step, user A randomly chooses $l_A \in_r \mathbb{Z}_q^*$ and computes $M_A = l_A(S_A + q_A P_A)$. Then, this user transmits following message:

$$A \to Coalition_i: ID_A, S_A = s_A P, M_A, ID_B$$

This message shows the request of user A with identifier $ID_A$ for the public key of user B with identifier $ID_B$.

- **Step2**: In this step, coalition i randomly chooses $l_i \in_r \mathbb{Z}_q^*$ and computes $M_i = l_i(S_i + q_i P_i)$. Then, this coalition transmits following message:

$$Coalition_i \to A: < P_i, M_i, U, C, W, Y >$$

The coalition sends tuple $< P_i, M_i, U, C, W, Y >$ to A if this user has been mentioned in a trusted list. Here,

$P_i = d_i \mathrm{P}$, $U = S_i = s_i P$, $C = e_B \oplus H_2(g_i)$ that $g_i$ is equal to $g_i = l_i(s_i + q_i d_i) M_A$
$W = e_B . P$ and $Y = N_B \oplus H_3(e_B)$.

- **Step3**:

At this stage user A can gain $< e_B, N_B >$ via following computation;

$$g_A = l_A(s_A + q_A d_A) M_i$$
$$H_2(g_A)$$
$$e_B = C \oplus H_2(g_A)$$

Since, in order to extract the public-key correctly the values $g_A$ and $g_i$ must be equal, A can checks authenticity of the received public key via the equation $W = e_B . P$. If it does not hold then A will reject the received public key otherwise it will be accepted and A computes $N_B = Y \oplus H_3(e_B)$.

As mentioned above, the values $g_A$ and $g_i$ must be equal to have a correct scheme hence we prove our claim by the following calculations:

$$g_A = l_A(s_A + q_A d_A) M_i$$
$$= l_A(s_A + q_A d_A)[l_i(s_i + q_i d_i) P]$$
$$= l_i(s_i + q_i d_i)[l_A(s_A + q_A d_A) P]$$
$$= l_i(s_i + q_i d_i) M_A$$
$$= g_i$$

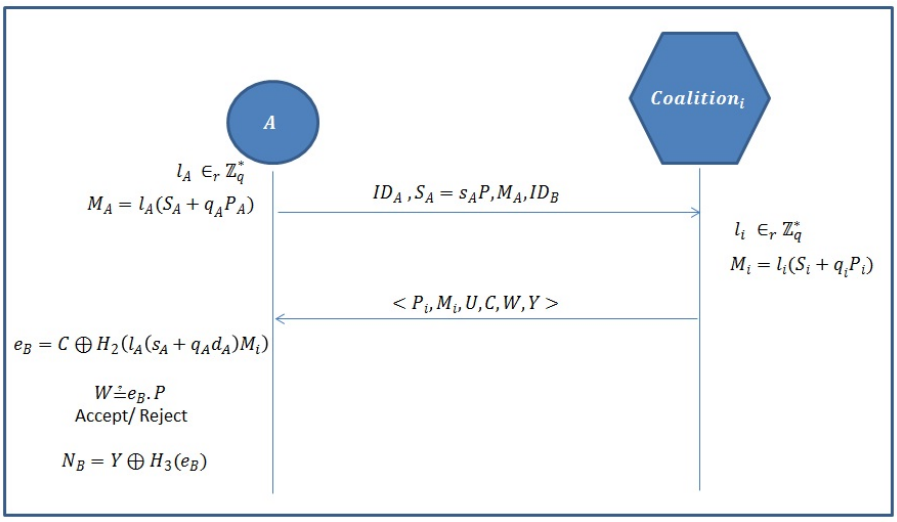


Figure 2. Public-key obtaining process

## V. COMPARISON

In this section we are going to show the superiority of our proposed protocol over IDRSA from complexity of computation perspective.

Due to this fact that the computation of $g_A$and $g_i$ values in public key obtaining process is foremost part in IDRSA and also our work, our focus for the comparison is just over this computation.

In our proposed scheme we have tried to decrease the computational cost via eliminating Bilinear Pairings operation. As shown in the Table 1, the pairing operation is significantly more expensive than other group operations [21]. In this table, the Type 1 of Bilinear Pairings is not considered due to the low security level (not more than 80 bits).

**Table 1.** Computational costs of operations inType2 and Type3 bilinear pairings [21]

| Group operation | Computational Cost | |
|---|---|---|
| | Type2 | Type3 |
| 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 |

Table 2 illustrates the overall computational cost of considered parts in IDRSA and our work.

**Table 2.** Overal computational costs of schemes

| Scheme | Computational Cost of operations |
|---|---|
| ID-RSA (Type2 pairings) | $E_T$+SM+2P |
| ID-RSA (Type3 pairings) | $E_T$+SM+2P |
| Our proposed scheme | 2SM |

Based on the information given in Table 1 and Table 2, the computational cost of IDRSA for Type2 and Type3 Bilinear Pairings is equal to 46 and 44 respectively while this value is only 2 for our scheme.

As a result, our scheme is more lightweight than IDRSA and it would be more appealing to be used in resource constrained environments like MANETs.

## VI. CONCLUSION

In this paper, we proposed a lightweight public key authentication scheme for resource constrained mobile enviornments such as Ad-hoc networks. Through eliminating the use of bilinear pairings and performing elliptic curve based algebraic groups, the results show that our proposed scheme is considerably more efficient from computational complexity perspective in compare with other related works especially IDRSA scheme.

## REFERENCES

[1] D. He, S. Padhye, J. Chen. (2012). "An efficient certificateless two-party authenticated key agreement protocol". Computers and Mathematics with Applications 64(6). Page 1914-1926.

[2] A. Shamir, (1984) “Identity-Based Cryptosystems And Signature Scheme”S, In Advances In Cryptology—Crypto 1984, Lecture Notes In Comput.Sci. 196, Springer-Verlag, Berlin.

[3] S.S.Al-Riyami K.G.Paterson. (2003) “Certificateless public key cryptography”. page 452-473. C.S. Laih (ed.) Advances in Cryptology C Asiacrypt 2003, Lecture Notes in Computer Science.

[4] G. Yang, C. Tan. (2011). “Strongly secure certificateless key exchange without pairing”. In: 6th ACM Symposium on Information, Computer and Communications Security. Page 71–79.

[5] Sun H, Wen Q, Zhang H, Jin Z. (2013). “A novel pairing-free certificateless authenticated key agreement protocol with provable security”. Frontiers of Computer Science. Page 544–557.

[6] A.W. Dent. (2006). “ A Survey of Certificateless Encryption Schemes and Security Models”. In: Cryptology ePrint Archive. Available online: http://eprint.iacr.org/2006/211

[7] B.C. Hu, D.S. Wong, Z. Zhang , X. Deng. (2007). “Certificatelss signature: a new security model and an improved generic construction”. Designs, Codes and Cryptography 42(2), 109–126.

[8] Z. Cheng, R. Comley. (2005). “Efficient certificateless public key encryption” ePrint Archive. Available online: http://eprint.iacr.org/2005/012/

[9] S. Capkun, L. Buttyan, and J. Hubaux. (2003). “Sector: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. Proc. of the ACM Workshop on Security of Ad Hoc and Sensor Networks.

[10] S. Yi, P. Naldurg, and R. Kravets, (2002). “Security-Aware Ad-hoc Routing for Wireless Networks”. Report No.UIUCDCS-R-2002-2290, UIUC.

[11] Y. Hu, A. Perrig, and D. Johnson. (2002). “Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks”. Proc. of IEEE INFORCOM.

[12] K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, (2002). “A Secure Routing Protocol for Ad Hoc Networks”. Proc. of IEEE International Conference on Network Protocols (ICNP), pp. 78-87.

[13] Y. Hu, D. Johnson, and A. Perrig. (2002). “SEAD: Secure Efficient Distance Vector Routing in Mobile Wireless Ad-Hoc Networks”. Proc. of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA’02), pp. 3-13, 2002.

[14] L. Tamilselvan and V. Sankaranarayanan, (2007)."Prevention of Blackhole Attack in MANET", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, pp. 21-26.

[15] S. Zhao, A. Akshai, R. Frost, X. Bai. (2011). “A survey of applications of identity-based cryptography in mobile ad-hoc networks”. IEEE Commun. Surv. Tutorials Early Access.

[16] L.B. Oliveira and R. Dahab, (2006). “Pairing-based cryptography for sensor networks,” presented at IEEE International Symposium on Network Computing and Applications, Cambridge, MA.

[17] 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. Per Sec ’05, IEEE, pp. 146-150.

[18] J. K. Liu, J. Baek, J. Zhou, Y. Yang, and J. W. Wong, (2010) “ Efficient online/offline identity-based signature for WSN, ” in Proc. IJIS, pp. 287-296.

[19] L. Li, Z. Wang, W. Liu, Y. Wang, (2011). "A Certificate less Key Management Scheme in Moblie Ad Hoc Networks", 7th International Conf. on Wireless Communications, Networking and Mobile Computing, pp 1-4, China.

[20] T. Eissa, S. A. Razak, M.A, Ngadi.. (2012). "A novel lightweight authentication scheme for mobile ad hoc networks". AJSE 37, 2179–2192.

[21] L. Chen, Z. Cheng, Np Smart. (2007). “Identity-Based Key Agreement Protocols From Pairings” .International Journal Of Information Security– Springer.