ATLANTIS PRESS

Advances in Intelligent Systems Research, volume 132

2nd International Conference on Modelling, Simulation and Applied Mathematics (MSAM 2017)

Remote Registration and Log-in Scheme for Mobile Networks with PIN Number

Binbin Yu[1,2], Liang Hu[1], Jianfeng Chu[1], Ling Chi[1] and Hongtu Li[1,*]

[1]College of computer science and technology, Jilin University, Changchun, China

[2]College of Information Technology and Media, Beihua University, Changchun, China

[*]Corresponding author

***Abstract*—In this paper, based on Scott's PIN scheme and Hu's private key distribution scheme, we proposed a new effective remote registration and log-in scheme for mobile networks and devices. In our article, we can guarantee the performance of the protocol for mobile networks and ensure the security of the private keys saved in mobile devices. Finally, we analyses our scheme and compare with Scott's and Hu's schemes through the experiment on ARM chips.**

Keywords-identity based cryptography; mobile networks; authentication ; private key distribution

I. INTRODUCTION

In the recent years, mobile networks have been a very active research area with the rapid development of wireless communication technology. The mobile devices and mobile networks have become an important part of our learning, working and living. Unfortunately, the majority of these communication environments are insecure, thus leading to the sensitive information might be intercepted by any unauthorized entity. As a result, security has become a big problem when a remote user attempts to access the services over any open networks. Authentication and key agreement is the representative approach to verify the legitimacy of a remote user and establish a session key between the communication parties.

Shamir [1] first introduced the notion of ID based public-key cryptosystem, which might lighten the certificate overhead compared with the other public-key systems. Since then ID based key agreement schemes combining pairings have been presented [2]. However, the above schemes are not efficient applying for resource-constrained mobile devices due to the need for multiple pairing operations [3].

With the tremendous development of the network technologies, recently ID based authentication and key agreement schemes using elliptic curve cryptosystem (ECC) have been broadly deployed in the wireless networks for mobile devices. As compared with traditional

cryptosystem, ECC offers equivalent security with smaller key size. In 2009, Yang-Chang [4] proposed an efficient and practical ID based two-party mutual authentication scheme employing ECC. They both consider ID-based and ECC properties simultaneously. However, both Yoon-Yoo [5] and Islam-Biswas [6] discovered that Yang-Chang's two-party scheme had some security flaws such as suffered from impersonation, replay attacks and did not provide the session key forward secrecy. To resolve these problems, Yoon-Yoo and Islam-Biswas respectively proposed their effective enhancements with higher security. In 2014, Farash-Attari [7] also presented an effective enhancement over Chou's scheme [8] with more security. Recently Lu[9] point out that Farash-Attari's scheme vulnerable to trace attack and do have the problem of clock synchronization and improves Farash-Attari's scheme.

Scott[10] proposed an authenticated ID-based key exchange and remote log-in scheme with two-factor. Such a scheme is clearly open to the following active insider attack. In 2010, Hu [11] published a Registration and private key distribution protocol based on Identity based encryption to transfer private key to new user.

In this paper, based on Scott and Hu's works, we propose an effective remote registration and authentication scheme for mobile networks.

The reminder of this paper is organized as follows. Section 2 gives brief information about the underlying definitions and the schemes of Hu and Scott. We present our proposed scheme and its analysis in Section 3 and Section 4. Section 5 is a brief conclusion.

II. PRELIMINARIES

In this section, we will briefly review some definitions and Scott's and Hu's works.

A. Bilinear Maps

Let G_1, G_2 be two additive cyclic groups of prime order q and G_T be a multiplicative cyclic groups of prime order q. Let g_1, g_2 be the generator of G_1 and G_2, and e be a bilinear map, $e : G_1 \times G_2 \rightarrow G_T$ with the following properties:

- Bilinearity: for any $P_1 \in G_1$, $P_2 \in G_2$ and $a, b \in F_q^*$, we have $e(aP, bQ) = e(P, Q)^{ab}$.
- Non-degeneracy: $e(P, Q) \neq 1$.

- Computability: there exist an efficient algorithm to compute e.

If the same group is used for the first two groups (i.e. $G_1 = G_2$), the pairing is called symmetric and is a mapping from two elements of one group to an element from a second group. This is called Type 1 pairing. If group G_1 and G_2 are not the same, but there is an efficiently computable homomorphism $\phi : G_2 \rightarrow G_1$. The pairing is named Type 2. Type 3 pairing is that group G_1 and G_2 are not the same and there is no efficiently computable homomorphism between G_1 and G_2.

B. Bilinear Diffie-Hellman Problem

Most of the Pairing based Cryptography applications rely on the hardness of Bilinear Diffie-Hellman problem for their security: Given $P_1 \in G_1, P_2 \in G_2, aP_1, bP_1, cP_1, aP_2, bP_2, cP_2$ for any $a, b, c \in F_q^*$, compute $e(P, Q)^{abc}$. This problem depends on the hardness of the Diffie-Hellman problem.

C. Scott's PIN Scheme

In Scott's scheme, the algorithm reconstructs the individual secret from the large number stored on the hardware token and the PIN. It is important that a correct individual secret cannot be detected from its format--it is just a number, and any number is possible. Essentially the relationship is linear and of the form $D = N + PIN$, where D is the individual secret, and N is the number on the token.

For individuals to register with the trusted authority users must prove their identity ID. In return they are supplied with I and their individual secret sI where $I = H(ID)$, a point of order q on the curve. They store on their hardware token I and $(s - \rho)I$, where ρ is their personal choice of PIN number. The protocol is illustrated as Fig 1:

Alice	**Bob**
Generates random $a < r$	Generates random $b < r$
$ID_a \rightarrow$	$\leftarrow ID_b$
$B = H(ID_b)$	$A = H(ID_a)$
$P_a = \hat{e}_r((s-\alpha)A + \alpha A, B)^a$	$P_b = \hat{e}_r((s-\beta)B + \beta B, A)^b$
$P_a \rightarrow$	$\leftarrow P_b$
If $P_b \leq 1$ or $P_b{}^r \neq 1$ Abort	If $P_a \leq 1$ or $P_a{}^r \neq 1$ Abort
Key $= P_b{}^a = \hat{e}_r(A, B)^{sab}$	Key $= P_a{}^b = \hat{e}_r(B, A)^{sab}$

FIGURE I. SCOTT'S SCHEME

D. Hu's Scheme

The Hu's scheme is defined as followed in Figuer 2 as example:.

1) PKG chooses a large k-bit prime p such that p=2mod3 and p=6q−1 for some prime q>3. Let E be the elliptic curve defined by y2=x3+1 over Fp. Choose an arbitrary P∈E/Fp of order q. Pick a random number s∈ Zq and set Ppub= sP. Choose a cryptographic hash function H: for some n. Choose a cryptographic hash function G :{ 0, 1}→Fp. The message space is M= {0, 1}n. The cipher text space is C=E/Fp × {0,1}n. The system parameters are params=<p, n, P, Ppub, G, H>. The master-key is s ∈Zq.*

2) Alice picks a random number xA as a part of his private key, and sends his registered information to PKG by follow steps:

a) Alice computes: PA= xAP as the authentication when she login the IBE system and chooses a ∈Zq randomly. Then Alice computes c=H(aPA) and sends aPA and QA the public key of Alice to PKG.

b) PKG computes d=H(PAlice)=H(aPA) and chooses b from Zq randomly. Then PKG computes: TP=bP, and sends TP to Alice.

3) Alice computes: k1=e (cPPub, axATP).

4) PKG computes: k2=e (bPAlice, dPPub).

5) The shared secret session key is: K=H(QA||PPub||k1)=H(QA ||PPub||k2).

6) PKG sends the private key sQA to Alice by encryption with K.

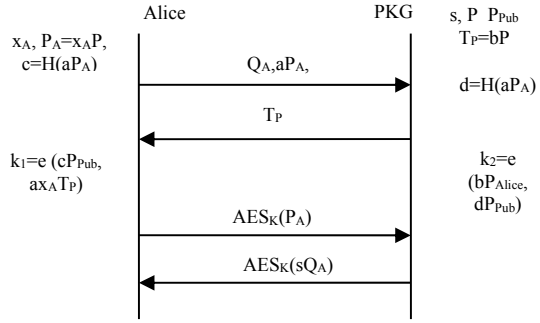

FIGURE II. HU'S SCHEME

III. REMOTE REGISTRATION AND LOG-IN SCHEME

As Scott's algorithm, we ensure safety of the user's privet key saving on the mobile device with the PIN. In our scheme, there are three parts: scheme Initialization, remote registration and remote log-in.

A. Scheme Initialization

The server end need initialize some parameters for the system. First, the server will be in possession of a master secret s, a random element of F_q. And the server keep the master secret itself. Then a user's private key could be computed as the form $sH(ID)$, where ID is the user identity and $H(\cdot)$ is a hash function which maps to a point on G_1. Here we assume that the hash function is modelled as a random oracle $H(ID) = r_{ID}P_1$ where $r_{ID} \in F_q$ is random and P_1 is a generator of G_1. The server will be issued with $P_{Pub} = sP_2$, where P_2 is a generator of G_2.

B. Remote Registration Algrithm

In this part, a user as a new customer could communicate with the server to get the token TOK which the user's private key is hiding by PIN. So, the user can store the TOK in mobile device without fear of private key leakage.

For new user to register with the server, they must prove the ID and some temporary parameters. In return the user is supplied with private key, a point on the curve. Then the user store on the mobile device $TOK = sA - I$, where I is the personal choice of PIN as Fig 3.

1) The user picks a random number $x \in Z_q^*$, and computes $U = xP_{Pub}$. Then the user sends the params ID and U to server. Here the user need not wait for the answer of server. He or she could get a session key by computing $K = H_k(G, ID)$ where G is get from $G = e(xA, P_{Pub})$.

2) The server gets the ID of a user and U. Then server could compute private key for user with follow steps:

a) The server get the map of ID by computing $A = H(ID)$. *Then compute the private key with master key.*

b) To ensure transfer the private key to user safley, the server need compute a session key to ecrypt the private key. First, compute $V = s^{-1}U$, *and* $G = e(sA, V)$. *Afler that, server computes session key as* $K = H_k(G, ID)$. *Now encrypt the private key using symmetric cryptographic，like AES.*

3) Getting the cipher from server, the user could decrypt the information, and obtain the private key sA. Then user save the token $TOK = sA - I$ where $I = H(PIN) \in G_1$.

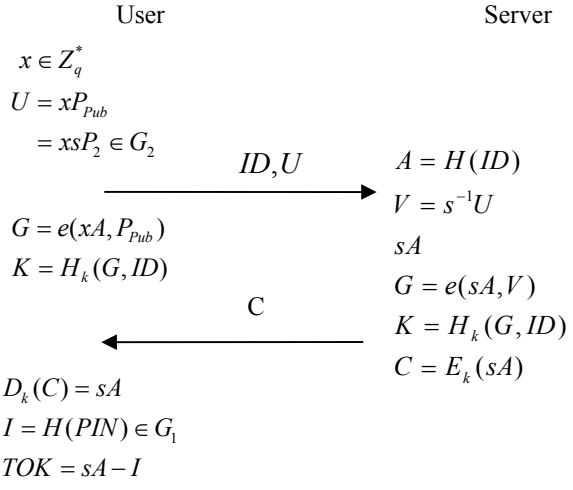

FIGURE III. REMOTE REGISTRATION ALGRITHM

C. Remote Log-in Algrithm

When a user gets the token TOK stored in the mobile device, he can remotely log-in the system as follow:

1) The user picks a random nmber $r \in Z_q^*$,and maps the ID and time stamp T_i to points as $A = H(ID)$ and $T = H(T_i)$. After that add the point A to T. Then compute $U = rD$, $W = rA$ where D is the sum of A and T. Now user send ID, U, W to server.

2) Server gets a number y randomly, and computes $sT = sH(T_i)$ where T_i is time stamp of server and s is the master key.

3) User receives the information from server, and send the resualt $V = -(x + y)(TOK + I + sT)$ where $I = H(PIN)$

4) Server verify the idenitity as Fig 4.

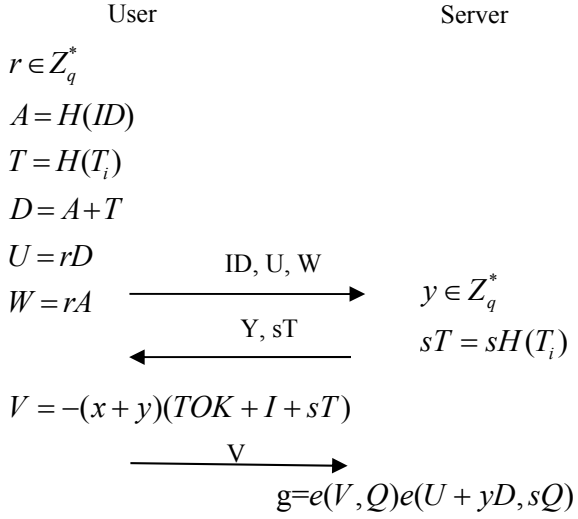

FIGURE IV. REMOTE LOG-IN ALGRITHM

IV. SCHEME ANALYSIS

In this section, we will give a brief analysis of our scheme.

A. Security Analysis

Our scheme is based on BDH problem. If an adversary can broke the scheme just with the public transport information，he can dill with the BDH problem.

In mobile networks a user may run the scheme on mobile device, and if the user lost his device, he doesn't need to worry about the private key. Because there is no private key in the device, but the token number.

B. Efficiency Analysis

We will compare the performance and functionality of our scheme with other related schemes. To estimate accurately for the running time, we use the MIRACL library to perform the cryptographic primitives for thousand executions and take the arithmetic mean based on 120MHz ARM chip.

TABLE I. COMPARE AND ANALYSIS

	Scott	Hu	Our
Whole scheme cost	≈ 2.1s	≈ 1.5s	≈ 1.8s
User end cost	≈ 1.1s	≈ 0.8s	≈ 0.7s
Support registration	x	√	√
Support Authentication	√	x	√
Support key agreement	√	√	x

V. CONCLUSION

In this paper, we have shown the schemes of Scott and Hu. Then we proposed a new effective remote registration and log-in scheme for mobile networks and device. Ensure the security of the private key saved in mobile device. And we analyses and compare with some other schemes.

ACKNOWLEDGMENT

This work is funded by: European Framework Program (FP7) under Grant No. FP7-PEOPLE-2011-IRSES, and by National Natural Science Foundation of China under Grant No. 61073009, and by National Sci-Tech Support Plan of China under Grant No. 2014BAH02F03, and by Youth Science Foundation of Jilin Province of China under Grant No. 20160520011JH.

REFERENCES

[1] A. Shamir, “Identity-based cryptosystems and signature schemes,” Advances in Cryptology-CRYPTO’84, Springer, New York, pp. 47-53, 1985.

[2] M. Holbl, T. Welzer, B. Brumen, “An improved two-party identity-based authenticated key agreement protocol using pairings,?Journal of Computer and System Sciences, vol. 78, pp. 142-150, 2012.

[3] X.F. Cao, W.D. Kou, Y.U. Yu, R. Sun, “Identity-based authentication key agreement protocols without bilinear pairings,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. 91, no. 12 , pp. 3833-3836, 2008.

[4] J.H. Yang, C.C. Chang, “An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem,” Computers & security, vol.28, no. 3, pp. 138-143, 2009..

[5] E.Yoon, K.Yoo, “Robust ID-based remote mutual authentication with key agreement protocol for mobile devices on ECC,” in Proc. of 2009 international conference on computational science and engineering, pp. 633-640, 2009.

[6] S.H. Islam, G.P. Biswas, “A more efficient and secure ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem,” Journal of Systems and Software, vol.84, no.11, pp. 1892-1898, 2011.

[7] M.S. Farash, M.A. Attari, “A secure and efficient identity-based authenticated key exchange protocol for mobile client–server networks,” The Journal of Supercomputing, vol. 69, pp. 395-411, 2014.

[8] C.H. Chou, K.Y. Tsai, C.F. Lu, “Two ID-based authenticated schemes with key agreement for mobile environments,” The Journal of Supercomputing, vol.66, no.(2): 973–988, 2013.

[9] Y. Lu, L. Li, H. Peng, and Y. Yang, “Robust ID based mutual authentication and key agreement scheme preserving user anonymity in mobile networks”, KSII Transactions on Internet and Information Systems , 10(3):1273{1288, 2016

[10] M. Scott. Authenticated ID-based key exchange and remote log-in with simple token and PIN number. Cryptology ePrint Archive, Report 2002/164, 2002. Available at http://eprint.iacr.org/2002/164.

[11] L. Hu, H.T. Li, J.F. Chu, H.W. Li, W. Yuan. Registration and private key distribution protocol based on IBE. Proceedings of The 5th International Conference on Frontier of Computer Science and Technology, 2010, 420 - 423