Anonymity Using Trusted Center with Cascade Digital Signatures

Abdulameer Khalaf Hussain
Jaresh University-Jordan
abdulameer.hussain {at} yahoo.com

Abstract—**This paper presents a variant scheme for hiding the user's identity with a structured construction. This scheme depends on group signature. The group consists of different subgroups and the members of each subgroup have their own private and public keys which can then have contact with private and public keys of the manager of the group. The scheme provides identity hiding based on the cascade encryption that ensures more security. All public keys of the members are maintained in a secure repository in the group. The result of this work was encouraging as it provides a strong identity hiding by analyzing different requirements of strong group signatures.**

Keywords--- ***Anonymity, Group Signature, Cascade Encryption, Identity Hiding.***

I. INTRODUCTION

Anonymity is considered an important issue in the Internet to offer services such as anonymous channels. It is an important idea for example the work of[1] shows that the anonymous e-cash can be used to commit a perfect crime. For this reason primitives such as fair off-line cash [2, 3] were proposed where it is possible for an authority to manage anonymity and reveals the identities of the entities behind a certain transaction given that certain conditions are satisfied.

Many works of group signatures had been introduced to be a tool used to offer anonymity. Examples of such studies are found in [4-7]. In group signature there is a group manager to join users in order to obtain a credentiality and be able to recover a piece of information that leads to the identity of the signer.

Digital signatures schemes had been invented by Diffie and Hellman [8] and then formalized by Goldwasser, Micali and Rivest [9]. Digital signatures do not only provide the electronic equivalent of signing a paper document with a pen but also are an important building block for many cryptographic protocols such as anonymous voting schemes, e-cash, and anonymous credential schemes, to name just a few. Digital signatures can be designed using one-way functions [10]. The efficiency of such constructions requires the signer's secret key to change between invocations of the signing algorithm.

To provide more security of digital signatures it is important to use an ideal random function (so-called random-oracle model) such as the RSA [11], the Fiat-Shamir [12], and the Schnorr [13] signature schemes.

II. RELATED WORKS

A formal definition of the signer anonymity for digital signature is proposed in [14]. The researchers show that a signer anonymous signature scheme can be very useful by proposing a new anonymous key exchange protocol which allows a client Alice to establish a session key with a server Bob securely while keeping her identity secret from eavesdroppers. In this protocol, the anonymity of Alice is already maintained when Alice sends her signature to Bob in clear, and no additional encapsulation or mechanism is needed for the signature.

In [15], the generalized version of the ring signature scheme had been proposed, which makes it possible for k members to sign a message without revealing their identification to the verifier. In this proposal the author showed two implementations of such signature scheme; one is based on zero-knowledge proof of random self-reducible problems, and the other is based on the polynomial over a finite field. Similar to ring signature scheme, the anonymity of signers in these two schemes is unconditional. This means that the identifications of the signers are impossible even if unlimited computational resources are available.

Lee and Chang [16] proposed a user identification scheme with key distribution that maintains the user anonymity for distributed computer networks. Then Wu and Hsu [17] showed that the Lee-Chang scheme is insecure against impersonation and identity disclosure attacks because any adversary can plot an impersonation attack to masquerade as a service provider in order to exchange a session key with a user without being detected in the authentication protocol. Yang et al. [18] demonstrated a compromising attack whereby it is

possible for an adversary to derive the private keys of users who request services.

After these researches it is important to deal with anonymous issuer Chien, H. Y., Chen. C. H. [19] Viet. D. Q., Yamamura. A. and Tanaka. H [20] respectively proposed their authentication schemes. The first one deals with anonymous communication not user anonymity, and the latter uses password tables at the server side and needs a lot of exponential operations. The first authors pointed out the vulnerabilities of both Viet et al.'s and Shin et al.'s anonymous password-based authenticated key exchange protocols, and then proposed a new anonymous password-based authenticated key exchange (JZH) protocol Jing are Yang et al.[21].

Zhenchuan Chai et al. [22] also proposed an efficient password-based authentication method and key exchange (CHCL) scheme for preserving user's privacy, and they analyzed the security requirements of their new scheme. They tried to achieve user anonymity without using group or ring signature schemes. In [23], a proposal of an anonymous identification scheme had been suggested which is based on the zero-knowledge proof scheme of possessing a digital signature algorithm DSA and thus eliminates the security vulnerability well and owned sensational properties. It has the superior properties of authentication, anonymity and unlinkablity.

III. PROPOSED SYSTEM

This paper proposes a system that depends on RSA algorithm to generate the group signature. It consists of a manger of the group and different subgroups. Each subgroup maintains its public keys (of their members) in a secure repository. Also each member of the subgroup has its own private key (d_i). The signature of each member in each subgroup is generated by raising the message m using the private key (d_{si}) of that member and sent it to the executive-manger (EM) of his/her own subgroup. The executive manager raises the result by his/her own private key (d_{ei}). The generated message is sent to the manager of the group. Finally the manager of the group raised the final message by his/her private key (d_m). In this manner the original message m is encrypted cascaded to ensure more security and eventually it provides a strong method for hiding the identity of each member and also the identity hiding of each executive manager. This procedure represents the operations of the sender side.

The second step is that the manger sends the final generated signature to the receiver. At the receiver end, there is only the public key of the manger (e_m). The receiver decrypts the signature and the result is that the original message is encrypted twice with two private key, the upper one is for the executive-manager and the lower one is the private key of the member of that subgroup, so the identity of both are hidden. Then only manager can recover the identity of each subgroup and its members.

Each subgroup has its own prime numbers (p and q), their products (n=p*q) and other subsequent calculations. For such purpose each subgroup maintains the public keys in a protracted repository of that subgroup and they are not public for the receivers of its whole group. Figure 1 illustrates the structure of the proposed system.

Algorithm

Let G be the set of prime numbers; $G=\{p_1q_1,p_2q_2,.....p_nq_n\}$
Let N be the set of n (the product of p_i *and* q_i*);* $G=\{n_1,n_2,....n_n)$
Let D be the set of all private keys d_i *(the private key of each member in each subgroup) ;* $D= \{d_1,d_2,.....d_m)$
Let d_m *be the private key of the manger of the group*
Let d_{si} *be the private key of the ith subgroup manager*
Let m be the message
Let E be the set of all public keys e_i *(which is the public key of each member);* $E=\{e_1,e_2,....,e_n\}$
Let e_m *is the public key of the manger of the group*
Let e_{si} *is the public key of the ith subgroup manager*

Sender Operations
$S_1=m^{di} \bmod n$
$S_2=(S_1^{dsi}) \bmod n$
$S_3=(S_2^{dm}) \bmod n=((m^{di})^{dsi})^{dm}$

Receiver Operations
Received Signature $= S_3^{em} \bmod n$

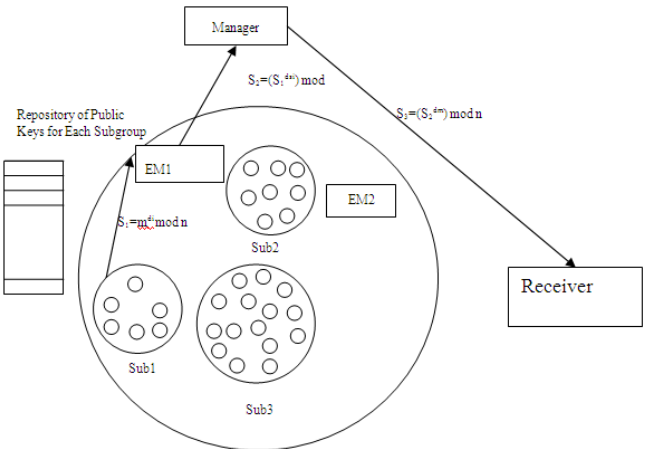

Figure 1: The structure of the Identity Hiding System

IV. RESULTS

Let $p_1=3$,$q_1=11$
$n_1=p_1*q_1=3*11=33$
$\Phi_1=(p_1-1)(q_1-1)=2*10=20$

Let e_1=7 such that GCD (e_1, Φ_1)=1 , GCD (7,20)=1
d_1=inv(e_1)mod Φ_1= 7^{-1} mod 20=**3**

Let p_2= 7, q_2=13
n_2=p_2*q_2=7*13=91
Φ_2=(p_2-1)(q_2-1)=6 *12=72
e_2= 5 , GCD (5,72) =1
d_2=inv(e_2) mod 72 = 5^{-1} mod 72
d_2= 5^{-1} mod 72 =29

Let p_3=23 q_3=37
n_3= p_3* q_3= 23*37= 851
Φ_3=(p_3-1)(q_3-1)=22 *36=792
e_3= 5 , GCD (5,792) =1
d_3=inv(e_3) mod 792 = 5^{-1} mod 792 =317

Let the shared message m=10;
S_1=10^3 mod 33= 10
S_2= 10^{29} mod 91= 82
S_3=82^{317} mod 851=578 (for Manager) the 82 is considered as a signature of all other parties)

Recovering of manager signature = 578^5 mod 851 =82

V. ANALYSIS &CONCLUSION

This paper presents an advanced method for hiding the identity of each user. The suggested method provides an anonymity for both members in each subgroup and also the identity hiding of their subgroups inside the whole group. So this method differs from other anonymity methods in that it hides the identity of the subgroup and their members.
Another important property of this method is that all public keys of both members and their corresponding subgroups are maintained in a secure repository inside the group. The group is controlled by a trusted manager who has the ability to monitor and control all operations and responsible for hiding the identity of all users including sub-groups executive-managers. In so doing, the anonymity parameter is **enhanced,** as given a message and its signature, the identity of the individual signer cannot be determined without the group manager's secret key.

If we analyze traceability parameter, this scheme provides an additional property of the traceability in that the group manager should be able to trace which user issued the signature in a hieratical manner instead of direct tracing. So we have two types of tracing, a direct one which is performed by each executive sub-group manager and indirect tracing related to the group manager.

Soundness and completeness of this scheme are more strong when they are compared with other schemes, where the validity of signatures of members are examined in one level, but in this scheme the signature issued by any member is checked at more levels from authorized managers.

Protecting members key especially public ones isolates each subgroup from other subgroups so the identity hiding is more complex when the keys are not protected as it is used in all identity hiding methods.

Finally the identity hiding is performed using the cascade encryption with multiple private keys (which is the basic of our structured identity scheme), because the cascade encryption is the most secure technique containing multiple ciphertext of the original message and thus facing most common attacks.

REFRENCES

[1] H .Sebastiaan, S.Von , and N.David," On blind signatures and perfect crimes. *Computers & Security*, 11(6):581–583, 1992.
[2] A.Giuseppe, C.Jan, J.Marc, and T.Gene , "A practical and provably secure coalition-resistant group signature scheme", In Mihir Bellare, editor, *CRYPTO 2000*, volume 1880 of *Lecture Notes in Computer Science*, pages 255–270. Springer, 2000.

[3] V. Yair, T.Yiannis, and Y.Moti, "Indirect Discourse Proof: achieving efficient fair off-line e-cash". In Kwangjo Kim and Tsutomu Matsumoto, editors, *ASIACRYPT 1996*, volume 1163 of *Lecture Notes in Computer Science*, pages 286–300. Springer, 1996.

[4] C. David ,and V.Eug`ene, "Group signatures" ,In *EUROCRYPT 1991*, pages 257– 265, 1991.

[5] C.Lidong , and P. Pedersen ,"New group signature schemes (extended abstract)", *EUROCRYPT 1994*, pages 171–181, 1994.

[6] A.Giuseppe , and M.Breno , "Efficient group signatures without trapdoors, In Chi-Sung Laih, editor, *ASIACRYPT 2003*, volume 2894 of *Lecture Notes in Computer Science*, pages 246–268. Springer, 2003.

[7] B. Dan , and S.Hovav ,"Group signatures with verifier-local revocation", In Vijayalakshmi Atluri, Birgit Pfitzmann, and Patrick Drew McDaniel, editors, *CCS 2004*, pages 168–177. ACM, 2004.

[8] D. Whitfield ,and E. Hellman, "New directions in cryptography", IEEE Trans. On Information Theory, IT-22(6):644–654, Nov. 1976.

[9] G. Shafi, M. Silvio, and R.Ronald, "A digital signature scheme secure against adaptive chosen-message attacks", SIAM Journal on Computing, 17(2):281–308, April 1988.

[10] N. Moni ,and Y. Moti , "Universal one-way hash functions and their cryptographic applications", Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing, pages 33–43, Seattle, Washington, 15–17 May 1989. ACM.

[11] L. Rivest, S. Adi, and L. Adleman , "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, 21(2):120–126, February 1978.

[12] A. Fiat and S.Adi , "How to prove yourself: Practical solution to identification and signature problems" Andrew M. Odlyzko, editor, Advances in Cryptology — CRYPTO '86, volume 263 of Lecture Notes in Computer Science, pages 186–194. Springer Verlag, 1987.

[13] P. Schnorr," Efficient signature generation for smart cards. Journal of Cryptology", 4(3):239–252, 1991.

[14] Y. Guomin , S. Wong , D . Xiaotie ,and H. Wang , " Anonymous Signature ,IN PUBLIC KEY CRYPTOGRAPHY (2006) , p: 347-363.

[15] H. Kuwakado ,and H .Tanaka , " Digital Signature Schemes with Anonymous Signers" **,** IEIC Technical Report (Institute of Electronics, Information and Communication Engineers) **VOL.**102;**NO.**212(ISEC2002 34-56);**PAGE.**95-100(2002) .

[16] W.B. Lee, and C.C. Chang , "User identification and key distribution maintaining anonymity for distributed computer network", Computer Systems Science and Engineering 15(4) (1999) 113-116

[17] T.S. Wu, and C.L. Hsu," Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks", Computers and Security 23 (2) (2004) 120-125.

[18] Y. Yang, S.Wang, F. Bao, J.Wang,and R.H. Deng," New efficient user identification and key distribution scheme providing enhanced security", Computers and Security 23 (8)(2004) 697-704.

[19] H.Y.Chien, and C.H.Chen , "A remote authentication scheme preserving user anonymity", Proceedings of the 19th International Conference on Advanced Information Networking and Applications-AINA 2005, 245-248

[20] D.Q.Viet, A.Yamamura,and H.Tanaka, "Anonymous password-based authenticated key exchange", Advances in Cryptology INDOCRYPT 2005, LNCS, Vol. 3797, Berlin: Spring-Verlag, (2005) 244-257

[21] J. Yang, and Z. Zhang, " A new anonymous passwordbased authenticated key exchange protocol",
INDOCRYPT 2008, LNCS 5365, pp.200-212, 2008, Springer-Verlag Berlin Heidelberg 2008

[22] Z. Chai, Z. Cao, and R. Lu, "Efficient password-based authentication and key exchange scheme preserving user privacy", WASA 2006, LNCS 4138, pp.467-477, 2006. Springer- erlag Berlin Heidelberg 2006

[23] W. shang-ping,W. yu-min,W. xiao-feng,and Z. ya-ling,Qin bo,"A Zero-Knowledge Proof Scheme of
Possessing a DSA Digital Signature",ACTA ELECTRONICA SINICA 2004，32（5）：878-880.