New Kind of Delegation-based Anonymous Authentication Scheme for Wireless Roaming Networks

Chun-Lin Jiang[1], Shi-Lan Wu[1], Ke Gu[2]

(Corresponding author: Chun-Lin Jiang)

School of Mathematics and Computer Sciences, Xinyu University[1]

Xinyu 338004, Jiangxi, China

(Email: 38029747@qq.com)

School of Computer and Communication Engineering, Changsha University of Science and Technology[2]

Changsha 410004, China

(Received Mar. 15, 2017; Revised and Accepted June 25 & July 13, 2017)

Abstract

In order to reduce message flows of traditional anonymous authentication schemes, a new kind of delegation-based scheme is proposed for wireless roaming networks. By making use of a proxy signature, the new scheme requires only a user and a visited server to participate in the authentication process, without the real-time participation of user's home server. Therefore, the new scheme needs less message flows than traditional schemes. In an instantiation of the new scheme, elliptic-curve cryptography (ECC) is used to keep efficiency, and the mobile station needs only 3.25 elliptic curve scalar multiplication (ECSM) operations, which are 5.5ECSM and 3Pairing less than the scheme based on group signature. The comparison shows that, though the unlinkability of our scheme is weaker, the computation load is much lower. So our scheme is efficient and practical.

Keywords: Anonymous Authentication; Delegation; Diffie-Hellman Key Exchange; Proxy Signature; Wireless Roaming Networks

1 Introduction

In wireless roaming networks, when a mobile station (MS) authenticates itself to a visited location register (VLR), the identity (ID) of MS is often valuable and must be protected. Because MS registers to its home location register (HLR), VLR often needs to communicate with HLR to authenticate MS, and MS also needs HLR to authenticate VLR.

The authentication process of most existing anonymous authentication protocols involves three parties including MS, VLR and HLR. According to the needed computational operations in MS, these traditional protocols are often divided into three types: (1) non-encryption based type that needs no cryptographic operations in MS [3, 22]; (2) secret-key based type that needs symmetric encryption operations in MS [9, 26]; (3) public-key based type that needs asymmetric encryption operations in MS [1, 6, 7, 10, 15, 25]. The first type often uses one-way hash functions and exclusive-OR operations to reduce the computation cost in MS, but it requires too many message flows (eight flows in [3]). The second type is a common type, but it cannot solve the non-repudiation and key management problems. The third type is a hotspot recently because it can provide non-repudiation and key management service, but it is computationally expensive even though hardware prices have fallen a lot. Besides, all three types need the real-time participation of HLR and require at least four message flows. It is well known that the bandwidth of wireless networks is limited, and VLR is often far from HLR, so the involvement of HLR often makes the communication time too long to bear.

Therefore, it is necessary to design authentication protocols involving only MS and VLR. Protocols based on group signatures [17, 24] or ring signatures [23] (actually a ring signature is a simplified group signature) can meet the requirement. In this kind of scheme, HLR is considered as the group manager of a group signature system and MS as a member of the group; when MS roams to VLR, MS signs messages on behalf of the group without showing its ID; by verifying the group signature, VLR is sure that MS is one valid user of HLR. Though this kind of scheme often needs only three message flows, it is still not practical for realistic applications because it is complex for MS to generate a group signature.

This paper proposes a new kind of delegation-based scheme which not only meets the requirement but also has good performance. The rest of this paper is organized as follows. Section 2 reviews some existing work on proxy signature. Section 3 introduces the system model of the new scheme. Section 4 gives two examples to instantiate the scheme. Finally, we analyze and conclude it in Sections 5 and 6.

2 Related Work

Mambo [16] gives a definition of proxy signature as follow.

Definition 1. *A proxy signature is a signature that is generated by a proxy signer on behalf of the original signer. It is often used in the following scenario: a manager delegates his/her signature authority to his/her trustworthy assistant in advance; when he/she is too far away to sign a document, the assistant has the power to sign it on behalf of the manager. It includes three types of delegation: full delegation; partial delegation; delegation by warrant.*

Proxy signatures were used to construct traditional anonymous authentication protocols involving three parties [2, 4, 5, 8, 11, 12, 13, 14, 19, 20, 21]. In 2005, Lee and Yeh [12] proposed an anonymous authentication protocol based on partial delegation for wireless communication system. Their protocol adopted the public-key system to achieve the security requirements and employed off-line authentication process to save authentication time. But Lee and Chang [11] showed that it could not achieve non-repudiation in off-line authentication process. They presented an improved protocol which not only avoided the weakness but also reduced the computation cost. In 2008, Tang *et al.* [19] proposed an efficient anonymous authentication protocol based on delegation by warrant for wireless networks. The protocol uses elliptic-curve cryptography (ECC) to ensure safety and efficiency. But in 2014, Kumar *et al.* [8] demonstrated that Tang-Wu's scheme did not achieve the user unlinkability. They then proposed a robust authentication model utilizing the biometric to get unlinkability.

The authentication process of the above protocols can be summarized as follows. First HLR authorizes MS the power to sign; when MS roams to VLR, MS computes a valid proxy signature without showing its real ID; then VLR verifies the legality of MS based on the public key of HLR; finally HLR authenticates VLR and generates a session key for MS and VLR. Just as mentioned above, the real-time participation of HLR results in many message flows: five flows are needed in [5], six flows are needed in [12, 11] and four flows are needed in [19, 8]. Actually HLR is removable with two reasons. Firstly, MS can also authenticate VLR by verifying the signature of VLR. Secondly, according to [24], the session key should be only known to MS and VLR, and should be derived from contributions of both of them; in particular, HLR should not generate it for them. So it is feasible and necessary to change these protocols to the scheme involving only MS and VLR.

3 System Model

Our new scheme is described as follows. first HLR delegates his signature authority to MS in advance; when MS roams to VLR, VLR computes an ordinary signature and sends it to MS; then MS authenticates VLR by verifying the signature; finally MS computes a valid proxy signature without showing its real ID and VLR authenticates MS based on the public key of HLR. During the authentication, a session key is derived from MS and VLR.

Our scheme is composed of three parts: Initialization, delegation, and authentication.

1) Initialization: Let ID_M, ID_V and ID_H be ID of MS, VLR and HLR respectively; $Sig()$ and $Verify()$ be the signing and verifying algorithms of an ordinary signature scheme such as digital signature algorithm (DSA); $PSig()$ and $PVerify()$ be signing and verifying algorithms of a proxy signature scheme respectively. VLR has a private/public key pair (x_V, y_V).

2) Delegation: HLR generates a pseudonym $alias$ and a proxy signing key x_p for MS. The proxy verifying key y_p, which is often HLR's public key, is put in public by HLR.

3) Authentication: When MS roams to VLR, the authentication process between MS and VLR is in Figure 1.

It is illustrated as follows.

1) MS sends $alias$ to VLR.

2) VLR generates an ordinary signature σ_v on message m_v, and sends (m_v, σ_v, ID_v) to MS.

3) MS verifies σ_v with VLR's public key y_v. If the signature is valid, MS computes a proxy signature σ_M on message m_M, and then sends (m_M, σ_M, ID_H) to VLR. Otherwise, it rejects the connection.

4) VLR verifies σ_M with y_p. If the signature is valid, it accepts the connection. Otherwise, it rejects the connection. During the authentication, a session key is derived from m_M and m_v.

4 Two Examples

4.1 An Example Based on Partial Delegation

Lee and Chang's protocol [11] includes on-line and off-line authentication processes. It uses a backward hash chain to ensure the security, but it still has some weaknesses.

4.1.1 Review of Lee and Chang's Protocol

Figure 2 is the protocol of Lee and Chang. The protocol is illustrated as follows.

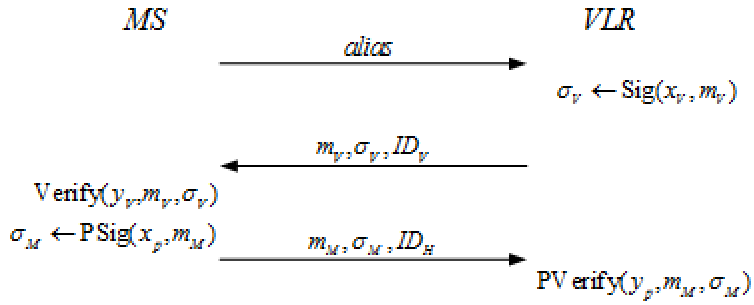

Figure 1: The authentication process of our model

1) Initialization: Let Z_p^* be a group of large prime order p, g be a generator of it, and q be a prime factor of $p-1$; K_{HV} be a shared key between HLR and VLR; (x, v) be a private/public key pair of HLR, with x a random number and $v = g^x \bmod p$; $[M]_K$ be the encryption of M using a symmetric key K; $h()$ be a one-way hash function; $||$ be a concatenation operator.

2) Delegation: First HLR generates a random number k and computes $\sigma = x + kK \bmod q$ as MS's proxy signing key and $K = g^k \bmod p$ as MS's pseudonym. Then HLR stores (σ, K) in its database and gives them to MS simultaneously.

3) On-Line Authentication:

   a. MS selects a random number n, pre-computes $h^{(i)}(n_1), h^{(2)}(n_1), \cdots, h^{(n+1)}(n_1)$ with $h^{(i)}(n_1) = h(n_1)$ and $h^{(i+1)}(n_1) = h(h^{(i)}(n_1))$ for $i = 1, 2, \cdots, n$. It then sends K to VLR.

   b. VLR selects a random number n_2 and sends (n_2, ID_v) to MS.

   c. MS selects a random number t, sets $N_1 = h^{(n+1)}(n_1)$, and then computes $r = g^t \bmod p$ and $s = \sigma h(N_1||n_2||ID_v) + tr \bmod q$ as the proxy signature. It then sends $(r, s, K, N_1, ID_H, ID_v)$ to VLR.

   d. VLR verifies the signature by checking $g^s = (vK^K)^{h(N_1||n_2||ID_v)} r^r \bmod p$. If the equation holds, VLR sends $([N_1||n_2||K]_{K_{HV}}, ID_H, ID_v)$ to HLR. Otherwise, VLR rejects the connection.

   e. HLR decrypts $[N_1||n_2||K]_{K_{HV}}$ and gets K. It then gets σ from its database and selects a random number n_3 to compute a session key $C_1 = h(N_1||n_2||n_3||\sigma)$ for VLR and MS. Finally HLR sets $l = N_1$ and sends $([[N_1, n_3, ID_v]_\sigma||n_2||l||C_1]_{K_{HV}}, ID_H, ID_v)$ to VLR.

   f. VLR gets $[N_1, n_3, ID_v]_\sigma||n_2||l||C_1$, checks (n_2, l), and accepts C_1 as the session key. Then VLR sends $([N_1, n_3, ID_v]_\sigma, ID_v)$ to MS.

   g. MS decrypts $[N_1, n_3, ID_v]_\sigma$, checks N_1 and computes the session key C_1.

4) i^{th} Off-Line Authentication:

   a. MS computes $[h^{(n-i+1)}(n_1)]_{C_1}$ and sends it to VLR for $i = 1, 2, \cdots, n$.

   b. VLR checks $h(h^{(n-i+1)}(n_1)) = l$, sets $l = h^{(n-i+1)}(n_1)$ and computes the session key $C_{i+1} = h(l, C_i)$. It then updates $i = i+1$ and checks $i \leq n$.

4.1.2 Analysis of the Protocol

The protocol is not efficient because it needs six message flows in on-line authentication process. It is also not secure because HLR knows the session key between VLR and MS.

4.1.3 Improved Protocol

Figure 3 is the improved protocol which is based on our model and is illustrated as follows.

1) Initialization: The same as original protocol. Besides, VLR has a key pair (x_v, y_v) of DSA.

2) Delegation: The same as original protocol.

3) On-Line Authentication:

   a. MS selects a random number n_1, pre-computes $h^{(i)}(n_1), h^{(2)}(n_1), \cdots, h^{(n+1)}(n_1)$ with $h^{(i)}(n_1) = h(n_1)$ and $h^{(i+1)}(n_1) = h(h^{(i)}(n_1))$ for $i = 1, 2, \cdots, n$. It then sends K to VLR.

   b. VLR selects a random number t_v and computes $n_2 = g^{t_v} \bmod p$. Then VLR computes a DSA signature σ_v on $n_2||ID_v$ and sends (n_2, σ_v, ID_v) to MS.

   c. MS verifies σ_v, selects a random number t and sets $N_1 = h^{(n+1)}(n_1)$. It then computes $r = g^t \bmod p$ and $s = \sigma h(N_1||n_2||ID_v) + tr \bmod q$ as the proxy signature. Finally MS sends $(r, s, K, N_1, ID_H, ID_v)$ to VLR and computes a session key $C_1 = n_2^t$.

   d. VLR verifies the signature by checking $g^s = (vK^K)^{h(N_1||n_2||ID_v)} r^r \bmod p$, if the equation holds, then VLR computes $C_1 = r^{t_v}$ and $l = N_1$. Otherwise, VLR rejects the connection.

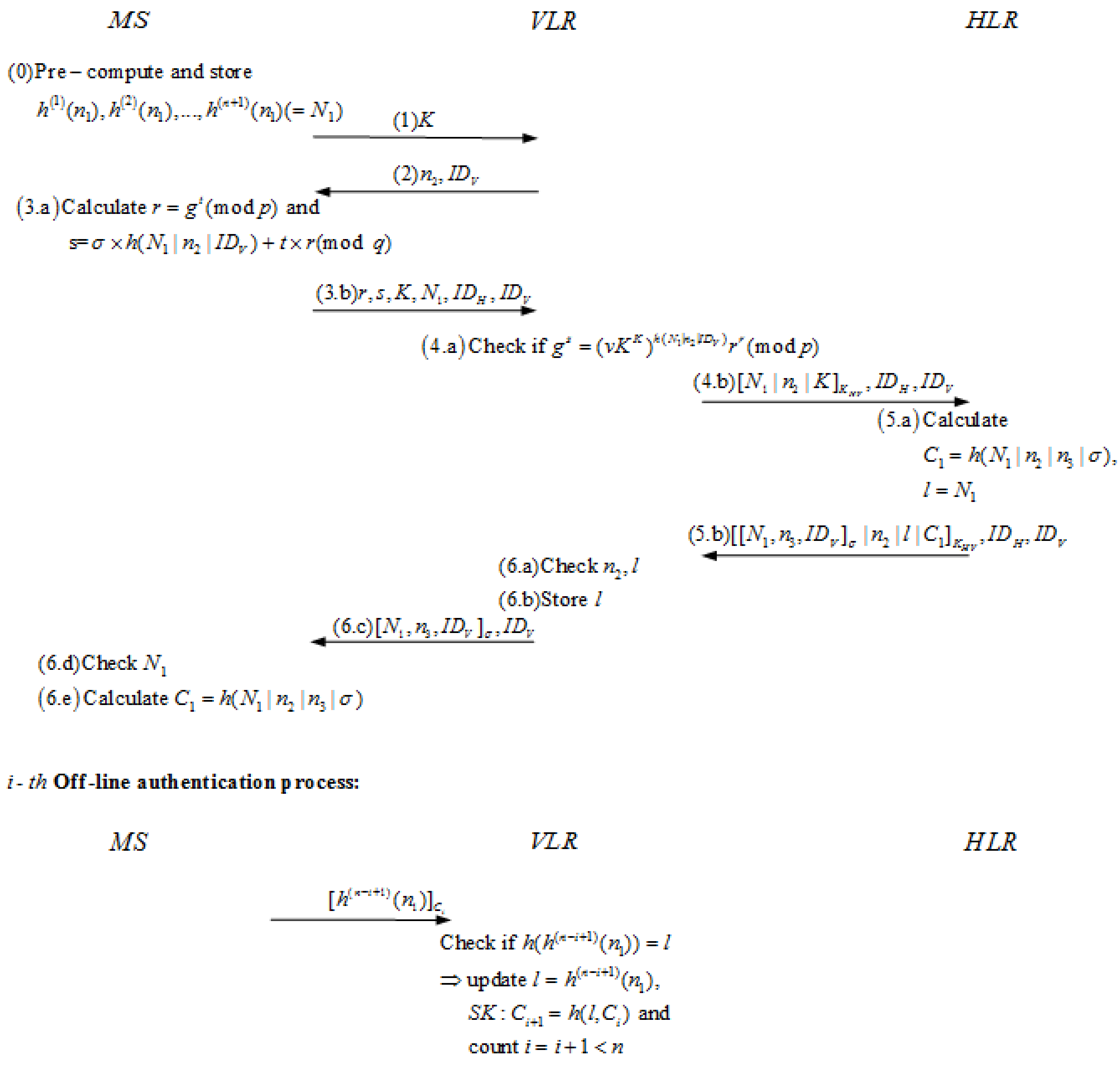

Figure 2: The authentication process of Lee and Chang

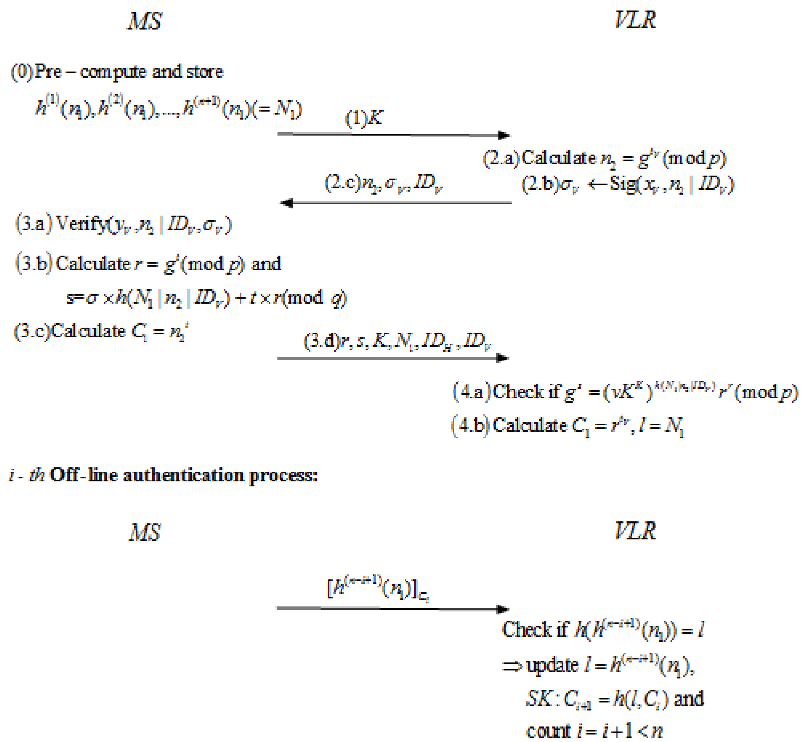

Figure 3: The improved authentication protocol

4) i^{th} Off-Line Authentication: The same as original protocol.

4.1.4 Performance Comparison

Table 1 is the performance comparison between original protocol and our improved protocol. Though MS needs one more calculation of public-key computation in our protocol, the message flows are greatly reduced from six to three in on-line authentication process. Besides, VLR and MS generate the session key based on Diffie-Hellman key exchange, which is secure under the decisional Diffie-Hellman (DDH) assumption. So our scheme is more efficient and secure.

4.2 An Example Based on Delegation by Warrant

In 2008, Tang *et al.* [18] proposed a proxy signature based on delegation by warrant by using an ECC system. We now combine this proxy signature with the elliptic curve digital signature algorithm (ECDSA) and the elliptic curve Diffie-Hellman (ECDH) exchange to design a really practical anonymous authentication protocol.

4.2.1 Description

Figure 4 is the protocol which is described as follows.

1) Initialization: Let F be a Galois field with an elliptic curve E in it, and T be a point of E; $(+)$ be a point addition operator in E; m_w be a warrant from which ID_M is not possible to be derived; Γ be public information used by VLR to verify MS; $\Pi()$ be a point representation function from E to Z_p; (x, Y) be a private/public key pair of HLR, with $x \in Z_p$ and $Y = xT$; (x_v, y_v) be an ECDSA private/public key pair of VLR; $h()$ be a secure hash function.

2) Delegation: HLR generates a pseudonym $IDMA = h(ID_M)$ for MS, selects a random number k and computes $\Gamma = (h(IDMA||m_w)T)(+)(kT)$ and $\sigma = -xh(\Pi(\Gamma)) - k$. Then HLR puts $(\Gamma, IDMA, m_w)$ in public, but delivers (σ, m_w) to MS secretly and securely. MS accepts the proxy signing key σ if $h(IDMA||m_w)T = (\sigma T)(+)(h(\Pi(\Gamma))Y)(+)\Gamma$.

3) Authentication:

   a. MS sends $IDMA$ to VLR.

   b. VLR selects a random number k_v, computes a ECDSA signature σ_v on $k_vT||ID_v$ and sends (k_vT, σ_v, ID_v) to MS.

   c. MS verifies σ_v, selects random numbers k and N, then computes $R = kT$ and $s = \sigma - kh(\Pi(R)||N)$ as the proxy signature. Finally MS sends (m_w, R, s, N, ID_H) to VLR and computes session key $C_1 = k(k_vT)$.

   d. VLR checks if (sT) $(+)$ Γ $(+)$ $(h(\Pi(\Gamma))Y)$ $(+)$ $(h(\Pi(R)||N)R) = h(IDMA||m_w)T$. If the equation holds, it then computes $C_1 = k_vR$ as

Table 1: Performance comparison between two protocols

Schemes	On/Off Line	Number of parties	Number of rounds	Number of secret-key computation in MS	Number of public-key computation in MS
Lee and Chang's protocol	On-line	3	6	1	1
	Off-line	2	1	n	0
Our improved protocol	On-line	2	3	1	2
	Off-line	2	1	n	0

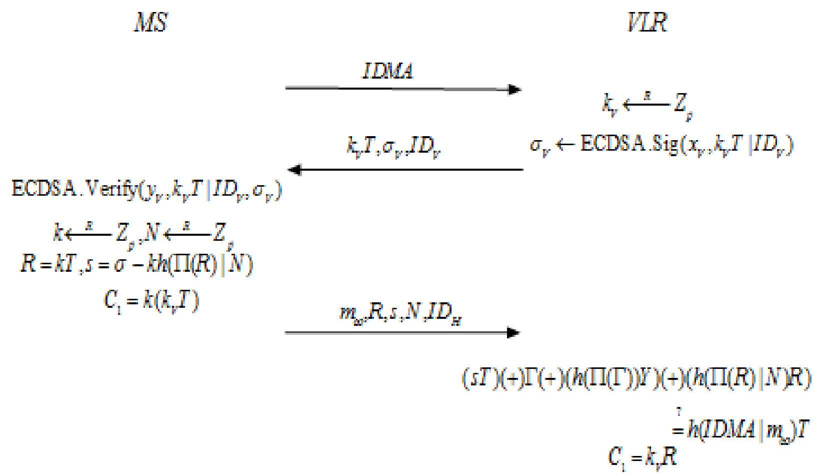

Figure 4: The protocol based on delegation by warrant

the session key. Otherwise it rejects the connection.

4.2.2 Comparison with the Scheme Based on Group Signature

In our scheme, MS does not send ID_M in plain text but a pseudonym instead. Anyone else including VLR cannot get ID_M. Unfortunately the pseudonym is generated by HLR, so MS cannot change it at will and can be easily traced. On the contrary, the protocol based on group signature in [24] can get strong unlinkability because the pseudonym is given by MS itself and can be changed arbitrarily. Though the unlinkability is weaker, our protocol is more efficient. Only 3.25 ECSM public key operations are needed by MS in our protocol, but 8.75 ECSM plus 3 Pairing operations are needed in [24]. Table 2 is the comparison between them. By using Table 3 from [24], we compare their computation delay in Figure 5, from which we can see that, our protocol needs only one fourth computation delay in [24].

Table 2: Comparison between [24] and our protocol

Schemes	Unlinkability	Public-key computation in MS
[24]	Strong	8.75ECSM+3Pairing
Our protocol	Weak	3.25ECSM

Table 3: Timings on 200MHz processor

	ECSM	Pairing
Time(ms)	23	38

5 Analysis

5.1 Security

In this section, we analyze our proposed scheme in terms of security.

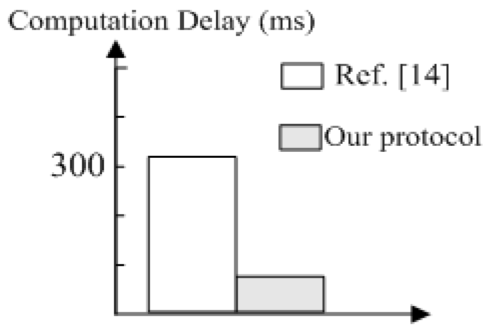

Figure 5: Computation delay in a 200MHz MS

1) Server authentication: In our scheme, MS is sure of the ID of VLR by verifying the signature of VLR.

2) Subscriber validation: MS signs a message on behalf of HLR; VLR verifies it to ensure that MS gets the delegation of HLR and is a valid user.

3) Key establishment: MS and VLR establish a common session key by Diffie-Hellman (DH) key exchange, which cannot be derived by anyone else including HLR.

4) User Anonymity: Besides the user and HLR, anyone else even VLR cannot tell the real identity of MS;

5) Resistance to man-in-the-middle attack: In our second example, an attacker cannot establish a fake Man-in-the-middle session key between MS and VLR because it is impossible for the adversary to get knowledge of the secret key k_v or k. The proposed protocol therefore resists the man-in-the-middle attack.

6) Non-repudiation: In our first example, MS will transmit $h^{n-i+1}(n_1)$ to VLR at the offline authentication phase. The $h^{n-i+1}(n_1)$ is a proof that MS requested VLR's service. Since it's based on hash chain irreversible characteristic, although VLR has the $h^{n_i+2}(n_1)$, which is received from previous communication, it still cannot generate the $h^{n-i+1}(n_1)$ by itself.

5.2 Practicability

In wireless roaming networks such as Cellular Networks, users often roam frequently. When users roam from one visited network to another, re-authentication is inevitable. Too much authentication time will affect the quality of service (QoS), especially in real-time interpersonal communications. Our scheme needs fewer message flows and less computation delay than traditional schemes and the scheme based on group signature respectively. Of course its unlinkability is weaker, which makes it not very satisfactory. But as an option, users can choose it if the bandwidth is not good or their mobile stations are not very powerful.

5.3 Disadvantages

Although our scheme is efficient in real-time interpersonal communications, it still has some disadvantages which may affect its application.

Weaker unlinkability is the first disadvantage which has been discussed above.

The second weakness of our scheme is its complex billing mechanism which is common in two-party protocols without involving HLR. One practical solution is the so-called "D-Coin" billing mechanism which employs the hash-chain technique. This has been discussed and solved in [27].

6 Conclusions

This paper introduces a new kind of delegation-based scheme involving only two parties. It is not only more secure and efficient than these schemes involving three parties, but also more efficient than the scheme based on group signature. Though its unlinkability is weaker, its high efficiency makes it more practical in power-limited and band-limited wireless roaming networks.

Acknowledgements

This work is supported by Science and Technology Project Founded by the Education Commission of Jiangxi Province (No. GJJ161195), Humanities and social science project of universities and colleges of Jiangxi Province (No. JC162001), Science and Technology Project Founded by the Xinyu science and Technology Bureau (No. 20163090862), and the National Nature Science Foundation of China (No. 61402055). The authors would like to thank the anonymous referees for their valuable suggestions.

References

[1] G. R. Alavalapati, A. K. Das, E. J. Yoon, *et al.*, "A secure anonymous authentication protocol for mobile services on elliptic curve cryptography", *IEEE Access*, vol. 4, pp. 4394-4407, 2016.

[2] M. K. Chande, C. C. Lee, C. T. Li, "Message recovery via an efficient multi-proxy signature with self-certified keys," *International Journal of Network Security*, vol. 19, no. 3, pp. 340-346, 2017.

[3] C. C. Chang, C. Y. Lee, Y. C. Chiu, "Enhanced authentication scheme with anonymity for roaming service in global mobility networks", *Computer Communications*, vol. 32, no. 4, pp. 611-618, 2009.

[4] L. Deng, H. Huang, and Y. Qu, "Identity based proxy signature from RSA without pairings," *International*

Journal of Network Security, vol. 19, no. 2, pp. 229-235, 2017.

[5] T. Gao, Q. Wang, X. Wang, *et al.*, "An anonymous access authentication scheme based on proxy ring signature for CPS-WMNs", *Mobile Information Systems*, Article ID 4078521, 11 pages, 2017.

[6] D. He, S. Zeadally, N. Kumar, *et al.*, "Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures", *IEEE Transactions on Information Forensics & Security*, vol. 11, no. 9, pp. 2052-2064, 2016.

[7] J. S. Kim, K. Jin, "Improved secure anonymous authentication scheme for roaming service in global mobility networks", *International Journal of Security & Its Applications*, vol. 6, no. 3, pp. 45-53, 2012.

[8] P. Kumar, A. Gurtov, J. Iinatti, *et al.*, "Delegation-based robust authentication model for wireless roaming using portable communication devices", *IEEE Transactions on Consumer Electronics*, vol. 60, no. 4, pp. 668-674, 2014.

[9] W. C. Kuo, H. J. Wei, J. C. Cheng, "Enhanced secure authentication scheme with anonymity for roaming in mobility networks", *Information Technology & Control*, vol. 43, no. 2, pp. 151-156, 2014.

[10] C. C. Lee, M. S. Hwang, I. Liao, "Security enhancement on a new authentication scheme with anonymity for wireless environments", *IEEE Transactions on Industrial Electronics*, vol. 53, no. 5, pp. 1683-1687, 2006.

[11] T. Lee, S. Chang, T. Hwang, *et al.*, "Enhanced delegation-based authentication protocol for PCSS", *IEEE Transactions on Wireless Communications*, vol. 8, no. 5, pp. 2166-2171, 2009.

[12] W. Lee, C. Yeh, "A new delegation-based authentication protocol for use in portable communication systems", *IEEE Transactions on Wireless Communications*, vol. 4, no. 1, pp. 57-64, 2005.

[13] L. H. Li, S. F. Tzeng, M. S. Hwang, "Generalization of proxy signature based on discrete logarithms", *Computers & Security*, vol. 22, no. 3, pp. 245–255, 2003.

[14] E. J. L. Lu, M. S. Hwang, and C. J. Huang, "A new proxy signature scheme with revocation", *Applied Mathematics and Computation*, vol. 161, no. 3, PP. 799-806, Feb. 2005.

[15] Y. Lu, X. Wu, X. Yang, "A secure anonymous authentication scheme for wireless communications using smart cards", *International Journal of Network Security*, vol. 17, no. 3, pp. 237-245, 2015.

[16] M. Mambo, K. Usuda, E. Okamoto, "Proxy signature for delegating signing operation", in *Proceedings of the 3rd ACM Conference on Computer and Communications Security*, pp. 48-57, 1996.

[17] A. Sudarsono, T. Nakanishi, Y. Nogami, *et al.*, "Anonymous IEEE802.1X authentication system using group signatures", *Journal of Information Processing*, vol. 18, pp. 63-76, 2010.

[18] C. Tang, D. Wu, "An efficient mobile authentication scheme for wireless networks", *IEEE Transactions on Wireless Communications*, vol. 7, no. 4, pp. 1408-1416, 2008.

[19] C. Tang, D. Wu, "Mobile privacy in wireless networks-revisited", *IEEE Transactions on Wireless Communications*, vol. 7, no. 3, pp. 1035-1042, 2008.

[20] S. F. Tzeng, M. S. Hwang, C. Y. Yang, "An improvement of nonrepudiable threshold proxy signature scheme with known signers", *Computers & Security*, vol. 23, no. 2, pp. 174-178, Apr. 2004.

[21] F. Wang, C. C. Chang, C. Lin, S. C. Chang, "Secure and efficient identity-based proxy multi-signature using cubic residues," *International Journal of Network Security*, vol. 18, no. 1, pp. 90-98, 2016.

[22] K. Y. Wu, K. Y. Tsai, T. C. Wu, *et al.*, "Provably secure anonymous authentication scheme for roaming service in global mobility networks", *Journal of Information Science & Engineering*, vol. 31, no. 2, pp. 727-742, 2015.

[23] Y. Xu, L. S. Huang, M. M. Tian, *et al.*, "Insecurity of a certificate-free ad hoc anonymous authentication", *International Journal of Network Security*, vol. 18, no. 5, pp. 993-996, 2016.

[24] G. Yang, Q. Huang, D. Wong, *et al.*, "Universal authentication protocols for anonymous wireless communications", *IEEE Transactions on Wireless Communications*, vol. 9, no. 1, pp. 168-174, 2010.

[25] K. H. Yeh, "An anonymous and lightweight autheniication scheme for mobile devices", *Information Technology & Control*, vol. 44, no. 2, pp. 206-214, 2015.

[26] H. Zhu, H. Li, W. L. Su, *et al.*, "ID-based wireless authentication scheme with anonymity", *Journal on Communications*, vol. 30, no. 4, pp. 130-136, 2009.

[27] H. Zhu, X. Lin, R. Lu, *et al.*, "Secure localized authentication and billing for wireless mesh networks", in *IEEE Global Telecommunications Conference (GLOBECOM'07)*, pp. 486-491, 2007.

Biography

Chun-lin Jiang received his Ph.D degree in the School of Information Science and Engineering from Central South University, China in 2012. His current research includes security and privacy of next generation wireless communication, protocols and heterogeneous networks.

Shi-Lan Wu received her M.S. degree in Hunan Normal University, Changsha, China, in 2011. She is now a teacher in Xinyu University. Her current research is protocols analysis.

Ke Gu received his Ph.D degree in the School of Information Science and Engineering from Central South University, China, in 2012. His current research includes information security and cryptography.