Int. J. of Computers, Communications & Control, ISSN 1841-9836, E-ISSN 1841-9844
Vol. V (2010), No. 4, pp. 586-591

Cryptanalysis on Two Certificateless Signature Schemes

F. Zhang, S. Li, S. Miao, Y. Mu, W. Susilo, X. Huang

Futai Zhang, Songqin Miao
1. School of Computer Science and technology
Nanjing Normal University,
Nanjing 210046, P.R. China, and
2. Jiangsu Engineering Research Center on Information Security and Privacy Protection Technology
Nanjing 210046, P.R. China
E-mail: zhangfutai@njnu.edu.cn, miaosongqin@163.com

Sujuan Li
1. School of Computer Science and technology
Nanjing Normal University,
Nanjing 210046, P.R. China, and
2. Nanjing University of Technology
Nanjing 210037, P.R. China
E-mail: lisujuan1978@126.com

Yi Mu, Willy Susilo, Xinyi Huang
Centre for Computer and Information Security Research
School of Computer Science and Software Engineering
University of Wollongong
NSW 2522, Australia
E-mail: ymu@uow.edu.au, wsusilo@uow.edu.au, xyhuang81@gmail.com

Abstract:
Certificateless cryptography has attracted a lot of attention from the research community, due to its applicability in information security. In this paper, we analyze two recently proposed certificateless signature schemes and point out their security flaws. In particular, we demonstrate universal forgeries against these schemes with known message attacks.

Keywords: certificateless cryptography, certificateless signature, public key replacement, universal forgery.

1 Introduction

Certificateless cryptography [1] is a new paradigm that not only removes the inherent key escrow problem of identity based public cryptography [2] (ID-PKC for short), but also eliminates the cumbersome certificate management in traditional PKI. In CL-PKC, the actual private key of a user is comprised of two secrets: a secret value and a partial private key. The user generates a secret value by himself, while the partial private key is generated by a third party called Key Generating Center (KGC), who makes use of a system wide master key and the user's identity information. In this way, the key escrow problem in identity-based public key cryptosystems is removed. A user's public key is derived from his/her actual private key, identity and system parameters. It could be available to other entities by transmitting along with signatures or by placing in a public directory. Unlike the traditional PKI, there is no certificate in certificateless public key cryptography to ensure the authenticity of the entity's public key. A number of certificateless signature schemes [3–14] have been proposed. Some of them are analysed under reasonable security models with elaborate security proofs [8, 11, 13, 14], while some others are subsequently broken due to flawed security proof or unreasonable model [3, 6–8, 12].

Recently two certificateless signature schemes were proposed in [4] and [5] respectively. They were claimed to provide high efficiency and provable security. In this short note, unfortunately, we show that these two schemes [4, 5] are insecure even in a very weak security model. Namely these two schemes are suffering from universal forgeries under known message attacks.

2 Review of the Original Schemes

We omit the preliminaries, basic notions, and security models about certificateless signature schemes. Please refer to [1, 8, 11, 13, 14] for details. The two original schemes [4, 5] are based on bilinear maps. They were both called McCLS scheme. To distinguish them, we call the one in [4] as McCLS1, and the other one in [5] as McCLS2.

2.1 Description of McCLS1

We first describe McCLS1. It consists of the following five algorithms.

- **Setup.** On input a security parameter, it generates a list of system parameters $\{ p, G_1, G_2, \hat{e}, P, P_{pub}, H_1, H_2\}$ and a system master private key $s \in Z_p^*$, where p is a large prime, G_1, G_2 are groups of order p with an admissible bilinear map $\hat{e}: G_1 \times G_1 \rightarrow G_2$, $H_1 : \{0,1\}^* \rightarrow G_1$ and $H_2 : \{0,1\}^* \rightarrow Z_p^*$ are cryptographical Hash functions, P is a generator of G_1, and $P_{pub} = sP$.

- **Extract Partial Private Key.** On input a user identity ID, it computes $Q_{ID} = H_1(ID)$, and outputs $D_{ID} = sQ_{ID}$ as the user's partial private key.

- **Generate Key Pair.** A user with identity ID selects a random $x \in Z_p^*$ as its secret value S_{ID}, and publish its public key $P_{ID} = xP_{pub}$.

- **CL-Sign.** Given a user's private keys (D_{ID}, S_{ID}) and a message M, the user randomly picks an element $r \in Z_p^*$, computes $S = {S_{ID}}^{-1} D_{ID}$, $R = (r - S_{ID})P$, $V = H_2(M, R, P_{ID})r$, and outputs $\sigma = (S, R, V)$ as his/her signature on message M under the public key P_{ID}.

- **CL-Verify.** Given a signature (S, R, V) on a message M of a user ID with public key P_{ID}, a verifier computes $h = H_2(M, R, P_{ID})$ and checks whether $(P_{pub}, VP - hR, h^{-1}S, Q_{ID})$ is a valid Diffie-Hellman tuple, namely whether the equation $\hat{e}(VP - hR, h^{-1}S) = \hat{e}(P_{pub}, Q_{ID})$ holds.

2.2 Description of McCLS2

The first three algorithms of McCLS2 in [5] are exactly the same as those of McCLS1 in [4]. There are slight differences in the **CL-Sign** and **CL-Verify** algorithms. We just depict the differences here.

- **CL-Sign.** Given a user's private keys (D_{ID}, S_{ID}) and a message M, the user randomly picks an element $r \in Z_p^*$, computes $S = {S_{ID}}^{-1} D_{ID}$, $R = (r - S_{ID})P$, $V = H_2(M, R, P_{ID})rP$ and outputs $\sigma = (S, R, V)$ as his/her signature on message M under public key P_{ID}.

- **CL-Verify.** Given a signature (S, R, V) on a message M of a user ID with public key P_{ID}, a verifier computes $h = H_2(M, R, P_{ID})$ and checks whether $(P_{pub}, V - hR, h^{-1}S, Q_{ID})$ is a valid Diffie-Hellman tuple, namely whether the equation $\hat{e}(V - hR, h^{-1}S) = \hat{e}(P_{pub}, Q_{ID})$ holds.

3 Universal forgery

As we can see, in the McCLS schemes, a signature on a message M of a user ID with public key P_{ID} consists of three components S, R and V. Note that for a user ID with public key P_{ID}, S remains unchanged for all messages, R and V are irrelevant to the partial private key D_{ID}. Here we give two kinds of universal forgery under known message attacks.

3.1 Attacks Against McCLS1

1. **Universal forgery by replacing public key**

   The scheme McCLS1 cannot resist public key replacement attacks of a type I adversary $\mathcal{A}$. For the definition of type I and type II adversaries, please refer to [1, 4, 5, 8, 11, 13, 14]. Let $\sigma = (S,R,V)$ be ID's valid signature on a message M, where

   $$S = {S_{ID}}^{-1} D_{ID},\ R = (r - S_{ID})P,\ V = H_2(M,R,P_{ID})r, \text{ and } r \in_R Z_p^*.$$

   Given R and V, the random number r can be easily derived as $r = VH_2(M,R,P_{ID})^{-1}$. And then $S_{ID}P$ is known as $S_{ID}P = rP - R$. Now $\mathcal{A}$ is able to forge a user ID's valid signature on any message m as follows:

   (a) Choose a random $c \in Z_p^*$ and let $r' = cr \in Z_p^*$;

   (b) Replace ID's public key as $P'_{ID} = cP_{ID}$ (the new secret value corresponding to the public key P'_{ID} is $S'_{ID} = cS_{ID}$);

   (c) Compute $S' = c^{-1}S, R' = cR, V' = H_2(m,R',P'_{ID})r'$;

   (d) Set $\sigma' = (S',R',V')$ as ID's signature on message m under the public key P'_{ID}. We can see that $(P_{pub}, V'P - H_2(m,R',P'_{ID})R', H_2(m,R',P'_{ID})^{-1}S', Q_{ID})$ is a valid Diffie-Hellman tuple since

   $$\begin{aligned}
   & \hat{e}(V'P - H_2(m,R',P'_{ID})R', H_2(m,R',P'_{ID})^{-1}S') \\
   = \ & \hat{e}((H_2(m,R',P'_{ID})crP) - H_2(m,R',P'_{ID})(crP - cS_{ID}P)), H_2(m,R',P'_{ID})^{-1}c^{-1}S) \\
   = \ & \hat{e}(H_2(m,R',P'_{ID})cS_{ID}P, H_2(m,R',P'_{ID})^{-1}c^{-1}S) \\
   = \ & \hat{e}(S_{ID}P, S) \\
   = \ & \hat{e}(P, D_{ID}) \\
   = \ & \hat{e}(P_{pub}, Q_{ID})
   \end{aligned}$$

2. **Universal forgery without replacing public key**

   From ID's valid signature $\sigma = (S,R,V)$ on a message M, the adversary can get

   $$r = VH_2(M,R,P_{ID})^{-1}, S_{ID}P = rP - R.$$

   With these he can forage a signature $\sigma' = (S',R',V')$ on any message m without replacing ID's public key as follows:

   Pick $r' \in_R Z_p^*$, and compute $S' = S$, $R' = r'P - s_{ID}P$, $V' = H_2(m,R',P_{ID})r'$.

   The verification will always output "accept" since

   $$(P_{pub}, V'P - H_2(m,R',P_{ID})R', H_2(m,R',P_{ID})^{-1}S', Q_{ID})$$

is really a valid Diffie-Hellman tuple. The reason is

$$\begin{aligned} & \hat{e}(V'P - H_2(m,R',P_{ID})R', H_2(m,R',P_{ID})^{-1}S') \\ = \; & \hat{e}(H_2(m,R',P_{ID})r'P - H_2(m,R',P_{ID})(r'P - S_{ID}P), H_2(m,R',P_{ID})^{-1}S) \\ = \; & \hat{e}(H_2(m,R',P_{ID})S_{ID}P, H_2(m,R',P_{ID})^{-1}S) \\ = \; & \hat{e}(S_{ID}P,S) \\ = \; & \hat{e}(P_{pub},Q_{ID}) \end{aligned}$$

3.2 Attacks Against McCLS2

1. **Universal forgery by replacing public key**

   Let $\sigma = (S,R,V)$ be ID's valid signature on a message M. It is obvious that

   $$rP = H_2(M,P,P_{ID})^{-1}V,\ S_{ID}P = rp - R.$$

   A type I adversary $\mathcal{A}$ may forge ID's valid signature on any message m as follows:

   (a) Choose a random $c \in Z_p^*$ and let $r' = cr \in Z_p^*$.

   (b) Replace ID's public key as $P'_{ID} = cP_{ID}$ (this implies the new secret value corresponding to the new public key P'_{ID} is $S'_{ID} = cS_{ID}$).

   (c) Compute
   $S' = c^{-1}S, R' = (r' - S'_{ID})P = cR, V' = H_2(m,R',P'_{ID})r'P = cH_2(m,R',P'_{ID})rP.$

   (d) Set $\sigma' = (S',R',V')$ as ID's signature on message m using public key P'_{ID}.
   We can see $(P_{pub}, V' - H_2(m,R',P'_{ID})R', H_2(m,R',P'_{ID})^{-1}S', Q_{ID})$ is a valid Diffie-Hellman tuple since

   $$\begin{aligned} & \hat{e}(V' - H_2(m,R',P'_{ID})R', H_2(m,R',P'_{ID})^{-1}S') \\ = \; & \hat{e}(H_2(m,R',P'_{ID})crP - H_2(m,R',P'_{ID})(crP - cS_{ID}P), H_2(m,R',P'_{ID})^{-1}c^{-1}S) \\ = \; & \hat{e}(H_2(m,R',P'_{ID})cS_{ID}P, H_2(m,R',P'_{ID})^{-1}c^{-1}S) \\ = \; & \hat{e}(S_{ID}P,S) \\ = \; & \hat{e}(P,D_{ID}) \\ = \; & \hat{e}(P_{pub},Q_{ID}) \end{aligned}$$

2. **Universal forgery without replacing public key**

   The adversary can get

   $$rP = H_2(M,R,P_{ID})^{-1}V,\ S_{ID}P = rP - R = H_2(M,R,P_{ID})^{-1}V - R,$$

   from ID's valid signature $\sigma = (S,R,V)$ on a message M. Then it (may be type I or type II) can forge a signature $\sigma' = (S',R',V')$ on any message m without replacing ID's public key as follows:

   Pick $r' \in_R Z_p^*$, and compute $S' = S$, $R' = r'P - s_{ID}P$, $V' = H_2(m,R',P_{ID})r'P$.

   The verification will always output "accept" since

   $$(P_{pub}, V' - H_2(m,R',P_{ID})R', H_2(m,R',P_{ID})^{-1}S', Q_{ID})$$

is really a valid Diffie-Hellman tuple. This is because

$$\begin{aligned} & \hat{e}(V' - H_2(m,R',P_{ID})R', H_2(m,R',P_{ID})^{-1}S') \\ = \; & \hat{e}(H_2(m,R',P_{ID})r'P - H_2(m,R',P_{ID})(r'P - S_{ID}P), H_2(m,R',P_{ID})^{-1}S) \\ = \; & \hat{e}(H_2(m,R',P_{ID})S_{ID}P, H_2(m,R',P_{ID})^{-1}S) \\ = \; & \hat{e}(S_{ID}P, S) \\ = \; & \hat{e}(P_{pub}, Q_{ID}) \end{aligned}$$

From these attacks, one can see McCLS1 and McCLS2 are insecure even in the weakest security model.

4 Conclusion

Recently, two certificateless signature schemes McCLS1 and McCLS2 were proposed for Mobile Wireless Cyber-Physical Systems. They only require two scalar multiplications in signing phase and two scalar multiplications and one pairing in verification phase. So they are efficient with respect to computational cost. Although the authors claimed and proved that McCLS1 and McCLS2 were secure, as we have shown in this paper they are in fact insecure. Universal forgeries against those two schemes have been presented under known message attacks.

5 Acknowledgment

This research is supported by the Natural Science Foundation of China under grant number 60673070 and Academic Discipline Fund of NJUT.

Bibliography

[1] S. Al-Riyami, K. Paterson. Certificateless public key cryptography. *Proceedings of Asiacrypt 2003*, Lecture Notes in Computer Science 2894, Springer-Verlag, 452-473, 2003.

[2] A. Shamir. Identity based cryptosystems and signature schemes. *Proceedings of Crypto'84*, 47-53, 1984.

[3] X. Huang, W. Susilo, Y. Mu, F. Zhang. On the security of a certificateless signature scheme. *Proceedings of ACISP 2005*, 13-25, 2005.

[4] Z. Xu, X. Liu, G. Zhang, W. He, G. Dai, W. Shu. A Certificateless Signature Scheme for MobileWireless Cyber-Physical Systems. *The 28th International Conference on Distributed Computing Systems Workshops*, 489-494, 2009.

[5] Z. Xu, X. Liu, G. Zhang, W. He. McCLS: Certificateless Signature Scheme for Emergency Mobile Wireless Cyber-Physical Systems. *International Journal of Computers, Communications & Control (IJCCC)*, 3(4): 395-411, 2008.

[6] W. Yap, S. Heng, B. Goi1. An efficient certificateless signature scheme. *Proceedings of EUC Workshops 2006*, Lecture Notes in Computer Science 4097, Springer-Verlag, 322-331, 2006.

[7] J. Park. An attack on the certificateless signature scheme from EUC Workshops 2006. *Cryptology ePrint Archive*, Report 442, 2006.

[8] Z. Zhang, D. Feng. Key replacement attack on a certificateless signature scheme. *Cryptology ePrint Archive*, Report 453, 2006.

[9] K. Choi, J. Park, J. Hwang, D. Lee. Efficient certificateless signature schemes. *Proceedings of ACNS 2007*, Lecture Notes in Computer Science 4521, Springer-Verlag, 443-458, 2007.

[10] R. Castro, R. Dahab. Two notes on the security of certificateless signatures. *Proceedings of ProvSec 2007*, Lecture Notes in Computer Science 4784, Springer-Verlag, 85-102, 2007.

[11] Z. Zhang, D. Wong, J. Xu, D. Feng. Certificateless public-key signature: security model and efficient construction. *Proceedings of ACNS 2006*, Lecture Notes in Computer Science 3989, Springer-Verlag, 293-308, 2006.

[12] B. Hu, D. Wong, Z. Zhang, X. Deng. Key replacement attack against a generic construction of certificateless signature. *Proceedings of ACISP 2006*, Lecture Notes in Computer Science 4058, Springer-Verlag, 235-346, 2006.

[13] X. Huang, Y. Mu, W. Susilo, D. Wong, W. Wu. Certificateless signature revisited. *Proceedings of ACISP 2007*, Lecture Notes in Computer Science 4586, Springer-Verlag, 308-322, 2007.

[14] L. Zhang, F. Zhang, F. Zhang. New efficient certificateless signature scheme. *Proceedings of EUC Workshops 2007*, Lecture Notes in Computer Science 4809, Springer-Verlag, 692-703, 2007.

Futai Zhang (b. Augest 28, 1965) received his M.Sc. in Mathematics (1990) from Shaanxi Normal University, China, and PhD in Cryptology (2001) from Xidian University, China. Now he is a professor at Nanjing Normal University, China. His current research interest is public key cryptography.

Sujuan Li is now a PhD candidate in Nanjing Normal University, China. Her current research interests include information security and cryptography.

Songqin Miao is now a M.Sc candidate in Nanjing Normal University, China. Her main research interest is cryptography.

Yi Mu received his PhD from the Australian National University in 1994. He is an associate Professor at the School of Computer Science and Software Engineering at the University of Wollongong. He is the co-director of Centre for Computer and Information Security Research (CCISR) at the University of Wollongong. His current research interests include network security, electronic payment, cryptography, access control, and computer security.

Willy Susilo received a Ph.D. in Computer Science from University of Wollongong, Australia. He is a Professor at the School of Computer Science and Software Engineering at the University of Wollongong. He is the co-director of Centre for Computer and Information Security Research (CCISR) at the University of Wollongong.His current research interests include information security and cryptography.

Xinyi Huang received his Ph.D. in Computer Science from University of Wollongong, Australia in 2009. His current research mainly focuses on cryptography and its applications.