Information Processing Letters 116 (2016) 416–418

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

On the security of two identity-based signature schemes based on pairings

Zhen Qin [a], Chen Yuan [a], Yilei Wang [a], Hu Xiong [a,b,*]

[a] School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, 610054, China
[b] State Key Laboratory of Cryptology, P.O. Box 5159, Beijing, 100878, China

ARTICLE INFO

Article history:
Received 28 December 2015
Accepted 17 February 2016
Available online 18 February 2016
Communicated by S.M. Yiu

Keywords:
Cryptography
Identity-based signature
Bilinear pairings
Forgery attack
Key disclosure attack

ABSTRACT

ID-based signature enables users to verify signatures using only public identifier. Very recently, Rossi and Schmid (2015) [9] proposed two identity-based signature schemes along with the application to group communications. Unfortunately, by proposing concrete attack, we demonstrate that the former scheme is insecure against forgery attack, while the latter scheme has been totally broken in the sense that the signing key can be recovered from the valid signature easily.

1. Introduction

As an essential and widely adopted cryptographic primitive, digital signature [8] offers the function of integrity, non-repudiation and authenticity. The notion of digital signature was initially proposed in the traditional asymmetric cryptosystem setting [4] such that users' public keys are calculated according to their corresponding secret keys. In this way, a trusted Certificate Authority (CA) is needed to issue the digital certificates to connect the public key and corresponding user. However, the management of public key certificates including generation, distribution, verification and revocation is historically considered as costly.

To eliminate the heavy certificate management in the traditional asymmetric cryptography, Shamir [10] introduced the innovative identity-based public-key cryptography (ID-PKC) in which the public identity (i.e., email address or social insurance number) of the user can be regarded as the public key of this user. Naturally, ID-based signature [5,7,12] has been proposed to enjoy the merits of signature and ID-PKC, and applied in different scenarios such as cloud computing [6], wireless sensor network [11] and secure routing [1].

Very recently, Rossi and Schmid [9] proposed two identity-based short signature schemes, namely IBS-1 and IBS-2, together with the application to authenticated group key agreement (GKA). Furthermore, the formal security proof of two identity-based signature schemes has also been given in the random oracle model. Specifically, Rossi and Schmid claimed that their two ID-based signature schemes achieve existential unforgeability under the co-CDH assumption [2]. Unfortunately, we observe that the former IBS-1 scheme is insecure against forgery attack and the signing key in the latter IBS-2 scheme can be recovered from the valid signature/message pair easily by the adversary. By considering the insecurity of their signature schemes, the authenticated group key agreement will be totally collapsed.

In the rest of this paper, we briefly review the identity-based signature schemes proposed by Rossi and Schmid [9] in Section 2. The analysis and discussions about the

* Corresponding author at: School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, 610054, China
E-mail address: xionghu.uestc@gmail.com (H. Xiong).

http://dx.doi.org/10.1016/j.ipl.2016.02.003
0020-0190/

weaknesses in Rossi and Schmind's schemes [9] are given in Sections 3 and 4. Finally, a conclusion is presented in Section 5.

2. Review of Rossi and Schmid's schemes

In this section, we briefly review Rossi and Schmid's identity-based signature schemes, namely IBS-1 and IBS-2 [9]. A trusted third party called key generation center (KGC) generates private signing key for every signer by using his/her identity.

2.1. Signature scheme IBS-1

In the scheme IBS-1, KGC and users perform the following steps to generate and to verify signatures.

Setup: During this step, KGC generates long-term parameters to prepare for the Key generation step.

1. KGC defines P to be a point of prime order l, where $gcd(l, q-1) = 1$. Then, KGC chooses the bilinear pairing e and the point P' which is linearly independent with the point P.
2. KGC generates the master signing key s and the master verification key V', where s is a random integer in $\mathbb{Z}_l^*$ and the V' equals sP'. Then, KGC chooses two functions $H : \{0,1\} \to \mathbb{G}$ and $h : \{0,1\} \to \mathbb{Z}_l^*$.
3. KGC publishes the public parameters (l, P, P', V') and the corresponding bilinear pairing e.

Key generation: KGC generates the signing key $S_1(id_A) = sH(id_A)$ based on user A's identity, where id_A is a free-text string.

Signing: The signer A chooses a random number r to compute $R' = rP'$ and $\Sigma = \frac{S_1(id_A)}{r+h(msg)}$, then $\{\Sigma, R'\}$ represents the signature for message msg.

Verification: After receiving the signature from user A, the verifier computes $H(id_A)$, $h(msg)$ and $R' + h(msg)P'$, then checks whether the equality (1) is true.

$$e(\Sigma, R' + h(msg)P') = e(H(id_A), V') \tag{1}$$

Verifier will accept the message and signature only if the equality holds.

2.2. Signature scheme IBS-2

In the scheme IBS-2, KGC and users perform the following steps to generate and to verify signatures.

Setup: The Setup algorithm is identical to the one in the signature scheme in Section 3.1.

Key generation: KGC generates the signing key $S_2(id_A) = \frac{P}{s+h(id_A)}$ based on user A's identity, and sends it to A secretly.

Signing: With message msg, the signer A chooses a random number r to compute $\Sigma = \frac{S_2(id)}{r+h(msg)}$ and $Q = r\Sigma$, then the tuple $\{\Sigma, Q\}$ represents the signature for msg.

Verification: After receiving the signature from user A, the verifier computes $H(id)$, $h(msg)$, $Q + h(msg)\Sigma$, $V' + h(id)P'$, then checks whether the equality (2) is true.

$$e(Q + h(msg)\Sigma, V' + h(id)P') = e(P, P') \tag{2}$$

Verifier will accept the message and signature only if the equality holds.

3. Analysis of Rossi and Schmid's schemes

In this section, we show that both the two signature schemes proposed by Rossi and Schmid [9] fail to achieve desirable properties. The first identity-based signature scheme IBS-1 in [9] is insecure against forgery attacks, and the second identity-based signature scheme IBS-2 has been totally broken such that anyone can disclose the signer's signing key with the valid message/signature pair.

3.1. The weakness of IBS-1 scheme

In the following, the adversary $\mathcal{A}$ can generate a valid signature on any message $msg_{\mathcal{A}}$ chosen by himself/herself under any user A's public identity id_A without the knowledge of this A's signing key.

Forging signature:

1. The adversary $\mathcal{A}$ chooses a pseudo-random integer r, computes $H(id_A)$ and $h(msg_{\mathcal{A}})$
2. $\mathcal{A}$ computes $R'_{\mathcal{A}} = \frac{V'}{r} - h(msg_{\mathcal{A}})P'$, and computes $\Sigma_{\mathcal{A}} = rH(id_A)$
3. After that, the forged signature for signer A on message msg is $(\Sigma_{\mathcal{A}}, R'_{\mathcal{A}})$.

After receiving the message $msg_{\mathcal{A}}$, identity id_A and the corresponding forged signature $(\Sigma_{\mathcal{A}}, R'_{\mathcal{A}})$, B verifies the validity of the signature $(\Sigma_{\mathcal{A}}, R'_{\mathcal{A}})$ on $msg_{\mathcal{A}}$ under the identity id_A as follows.

Verifying signature:

1. The verifier computes $H(id_A)$, $h(msg_{\mathcal{A}})$ and $R'_{\mathcal{A}} + h(msg_{\mathcal{A}})P'$
2. Then, B calculates and verifies the equality of equation (1):

$$\begin{aligned} &e(\Sigma_{\mathcal{A}}, R'_{\mathcal{A}} + h(msg_{\mathcal{A}})P') \\ &= e(rH(id_A), \frac{V'}{r} - h(msg_{\mathcal{A}})P' + h(msg_{\mathcal{A}})P') \\ &= e(H(id_A), V') \end{aligned}$$

It is trivial to generate a forged signature under the public verification key V' and A's identity id_A without the knowledge of A's signing key.

3.2. The weakness of IBS-2 scheme

In the identity-based signature scheme IBS-2, after receiving the one message/signature pair $\{msg, (\Sigma, Q)\}$ from signer A, the verifier B can recover A's private signing key $S_2(id_A)$ as follows:

1. According to the specification of the second ID-based signature scheme, the signature (Σ, Q) output by signer A on message msg is generated as $\Sigma = \frac{S_2(id_A)}{r+h(msg)}$,

$Q = r\Sigma$ such that r is a pseudo-random integer chosen by A and $S_2(id_A)$ denotes signer A's private signing key.

2. After receiving this messages/signature pair, the verifier B can disclose A's private signing key $S_2(id_A)$ successfully as follows:

$$\begin{aligned} Q + h(msg)\Sigma &= (r + h(msg))\Sigma \\ &= (r + h(msg))\frac{S_2(id_A)}{r + h(msg)} \\ &= S_2(id_A) \end{aligned}$$

4. Discussion

4.1. Our analysis

In [9], Rossi and Schmind claimed the security of their scheme are based on the assumptions in which BLS [3] and ZSS [13] are secure against adaptive chosen-message attacks. However, the algorithms of signature generation and verification in IBS-1 and IBS-2 are different from the ones in BLS [3] and ZSS [13]. Thus, the security of their schemes should be considered and proven from the hardness of co-CDH problem rather than the security of BLS [3] and ZSS [13].

The unforgeability of signature rests on the assumption in which only signer holds the signing key. In verification step of IBS-1, equation (1) is designed to reduce the part $(r + h(msg))$ in $(R' + h(msg)P')$ and denominator of Σ, and to verify the equation of $e(S_1(id_A), P') = e(H(id_A), V')$ by bilinearity property. However, the addition operation in $(R' + h(msg)P')$ leave a chance for $\mathcal{A}$ to bypass the verification. In the verification of forged signature $(\Sigma_{\mathcal{A}}, R'_{\mathcal{A}})$, $h(msg)P'$ is subtracted by the corresponding part $h(msg_{\mathcal{A}})P'$ in $R'_{\mathcal{A}}$ and the equation (1) still holds. Moreover, verifier cannot distinguish forged signatures from legal ones because of the participation of random number r. Thus, the forged signature $(\Sigma_{\mathcal{A}}, R'_{\mathcal{A}})$ computed from public parameters can be acknowledged by verifier successfully.

In the second scheme IBS-2, verifier should compute equation (2) to verify the correctness of signature (Σ, Q) on msg. In the calculation of equation (2), a intermediate equation will be generated:

$$e\Big(\frac{P}{s + h(id_A)}, (s + h(id_A))P'\Big) \stackrel{?}{=} e(P, P')$$

Obviously, the above equation can be transformed and proven to be true by bilinearity property. However, the $\frac{P}{s+h(id_A)}$ on the left side of equal is precisely the signer's signing key $S_2(id_A)$ defined in Section 2.2. This scheme is totally broken in the sense that everyone can recover the signing key from the signature easily.

4.2. About the application to group key agreement protocol

Group key agreement protocols are introduced to ensure the security of communications by establishing a shared session key among group members. In [9], Rossi and Schmid used the proposed identity-based signature schemes for the application of group key agreement. The signature schemes were adopted to authenticate messages exchanged with the aim of getting authenticated session keys. The confidentiality and integrality of group communications basically depends on the unforgeability of the signature schemes. By considering the weaknesses in the proposed signature schemes, the security of authenticated group key agreement is totally broken.

5. Conclusion

In this paper, we showed that two identity-based signature schemes proposed by Rossi and Schmid [9] are insecure against the forgery attack and key disclosure attack, which is contrary to the authors' claim. Furthermore, their group key agreement protocol based on their ID-based signature schemes is also not secure.

Acknowledgements

The authors would like to acknowledge National Natural Science Foundation of China under Grant Nos. 61003230, 61370026 and 61133016, the Fundamental Research Funds for the Central Universities under Grant No. ZYGX2013J073, and the National High Technology Research and Development Program of China (863) under Grant 2015AA016007. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] A. Boldyreva, C. Gentry, A. O'Neill, et al., Ordered multisignatures and identity-based sequential aggregate signatures, with applications to secure routing, in: Proceedings of the 14th ACM Conference on Computer and Communications Security, 2007, pp. 276–285.
[2] D. Boneh, B. Lynn, H. Shacham, Short signatures from the Weil pairing, in: C. Boyd (Ed.), Advances in Cryptology, ASIACRYPT 2001, Gold Coast, Australia, December 9–13, 2001, in: Lecture Notes in Computer Science, vol. 2248, Springer, Berlin, Germany, 2001, pp. 514–532.
[3] D. Boneh, B. Lynn, H. Shacham, Short signatures from the Weil pairing, J. Cryptol. 17 (4) (2004) 297–319.
[4] W. Diffie, M.E. Hellman, New directions in cryptography, IEEE Trans. Inf. Theory 22 (6) (1976) 644–654.
[5] F. Hess, Efficient identity based signature schemes based on pairings, in: Selected Areas in Cryptography, SAC 2002, Springer, 2002, pp. 310–324.
[6] H. Li, Y. Dai, L. Tian, et al., Identity-based authentication for cloud computing, in: Proceedings of the First International Conferenceon Cloud Computing, CloudCom, 2009, pp. 157–166.
[7] K.G. Paterson, ID-based signatures from pairings on elliptic curves, Electron. Lett. 38 (18) (2002) 1025–1026.
[8] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM 21 (2) (1978) 120–126.
[9] F. Rossi, G. Schmid, Identity-based secure group communications using pairings, Comput. Netw. 89 (2015) 32–43.
[10] A. Shamir, Identity-based cryptosystems and signature schemes, in: Advances in Cryptology, Springer, 1985, pp. 47–53.
[11] K.A. Shim, C.M. Park, A secure data aggregation scheme based on appropriate cryptographic primitives in heterogeneous wireless sensor networks, IEEE Trans. Parallel Distrib. Syst. 26 (8) (2015) 2128–2139.
[12] H. Xiong, Y. Chen, G. Zhu, Z. Qin, Analysis and improvement of a provable secure fuzzy identity based signature scheme, Sci. China Inf. Sci. 57 (9) (2014) 1–5.
[13] F. Zhang, R. Safavi-Naini, W. Susilo, An efficient signature scheme from bilinear pairings and its applications, in: Public Key Cryptography, PKC 2004, Springer, 2004, pp. 277–290.