HOSTED BY
ELSEVIER
CrossMark
Available online at www.sciencedirect.com
ScienceDirect
ICT Express 1 (2015) 94–95
www.elsevier.com/locate/icte

On the security of pairing-free certificateless digital signature schemes using ECC

Namita Tiwari

Department of Mathematics, Pranveer Singh Institute of Technology, Kanpur- 208001, India

Received 13 July 2015; received in revised form 28 November 2015; accepted 9 December 2015
Available online 15 December 2015

Abstract

I cryptanalyze the pairing-free digital signature scheme of Islam et al. which is proven secure against "adaptive chosen message attacks". I introduce this type of forgery to analyze their scheme. Furthermore, I comment on general security issues that should be considered when making improvements on their scheme. My security analysis is also applicable to other digital signatures designed in a similar manner.

Keywords: Digital signature; Certificateless cryptography; Elliptic Curve cryptography; Random Oracle model; Provable security

1. Introduction

Certificateless public-key cryptography solves the certificate management problem in traditional public-key cryptography, and solves the key-escrow problem in identity-based public-key cryptography. There are numerous certificateless signature schemes [1–8]. designed for different applications. To avoid bilinear pairing operations, Islam and Biswas [9] recently proposed a pairing-free certificateless digital signature scheme using elliptic curve cryptography (ECC). They also proved that their scheme was secure "against adaptive chosen-message and identity attacks" in the random oracle model. In this paper, I analyze the security of Islam et al.'s scheme and demonstrate that it is not secure even though it is proven secure against "adaptive chosen-message and identity attacks". Furthermore, I comment on general security issues that should be considered when making improvements on their scheme. The security of other similar schemes can be checked using the same techniques, I employed in our study.

The remainder of this paper is organized as follows. In Section 2, we discuss the security problem in Islam et al.'s [9] scheme. Section 3 presents the security heal. Finally, Section 4 concludes the paper.

E-mail address: namita.mnnit@gmail.com.

Peer review under responsibility of The Korean Institute of Communications Information Sciences.

2. Security analysis of Islam et al.'s scheme [9]

Adversary A can forge a valid signature on m by replacing the public key.

- After obtaining (ID_S, R_S), A randomly selects $d_A, x_A \in Z_q^*$, computes $P_A = x_A P$, $H_0(ID_S, R_S, P_A)$, $P'_{pub} = (d_A P - R_S){H_0}^{-1}$ and replaces master public key P_{pub} with P'_{pub} and ID_S's P_S with P_A so that $d_A P = R_S + H_0(ID_S, R_S, P_A) P_{pub}{}'$ holds.
- A sets (D_A, x_A) as full private key of the signer where $D_A = (d_A, R_S)$, and sets (P_A, R_S) as the full public key.
- To sign a message $m \in \{0, 1\}^*$, A selects $y_A \in_R {Z_q}^*$, computes $Y_A = y_A P_A$, $h_A = H_1(m, ID_S, R_S, Y_A)$ and $t_A = H_2(m, ID_S, P_A, Y_A)$.
  Finally A computes $\sigma_A = x_A y_A - (t_A x_A + h_A d_A) \bmod q$ and outputs the signature (σ_A, Y_A) on the message m.

Because $Y_A = y_A P_A = y_A x_A P, h_A = H_1(m, ID_S, R_S, Y_A)$, and $t_A = H_2(m, ID_S, P_A, Y_A)$.

Thus, $\sigma_A P = Y_A - t_A P_A - h_A(R_S + H_0(ID_S, P_A, R_S) P_{pub}{}')$.

Therefore, the generated signature can pass the verification, and A generates a signature successfully.

3. Formal proof to heal the security

When designing a signature protocol such as the one described above, the system public key P_{pub} should be hashed

http://dx.doi.org/10.1016/j.icte.2015.12.001

to eliminate the possibility of this type of forgery. A proposal to heal the security in [9] is given as follows.

- When executing Partial-Private-Key-Extract in [9], if P_{pub} is hashed in H_0, private key part d_i is computed as $d_i = (r_i + xH_0(ID_i, R_i, P_i, P_{pub})) \bmod q$ so that the user can validate their partial private key tuple $D_i = (d_i, R_i)$ by checking the equation $d_i P = R_i + H_0(ID_i, R_i, P_i, P_{pub})P_{pub}$.
- Now, after obtaining (ID_S, R_S), if A attempts to forge the signature in the same manner described in the previous section, it then randomly selects $d_A, x_A \in Z_q^*$, computes $P_A = x_A P$, $H_0(ID_S, R_S, P_A, P_{pub})$, $P'_{pub} = (d_A P - R_S)$ ${H_0}^{-1}$, and replaces master public key P_{pub} with P'_{pub} and ID_S's P_S with P_A.
- For the verification, one checks the equation $d_A P = R_S + H_0(ID_S, R_S, P_A, P'_{pub})P'_{pub}$, which will not hold. Therefore, forgery is not possible.

One can check the security of other proposed schemes that employ designs similar to the one described above.

4. Conclusion

In this paper, we have demonstrated that Islam et al.'s pairing-free certificate-less digital signature scheme is not secure against some forgery types even though it is proven secure against "adaptive chosen-message attacks". Furthermore, we commented on security issues to present a countermeasure.

References

[1] H. Chen, F.-T. Zhang, R.-S. Song, Certificateless proxy signature scheme with provable security, J. Softw. 20 (3) (2009) 692–701.

[2] D. He, Y. Chen, J. Chen, A provably secure certificateless proxy signature scheme without pairings, Math. Comput. Modelling 57 (9-10) (2013) 2510–2518.

[3] D. He, J. Chen, R. Zhang, An efficient and provably-secure certificateless signature scheme without bilinear pairings, Int. J. Commun. Syst. 25 (11) (2012) 1432–1442.

[4] X. Li, K. Chen, L. Sun, Certificateless signature and proxy signature schemes from bilinear pairings, Lith. Math. J. 45 (1) (2005) 76–83.

[5] R. Lu, D. He, C. Wang, Cryptanalysis and improvement of a certificateless proxy signature scheme from bilinear pairings, in: Proceedings of the 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, SNPD 07, Qingdao, China, July 2007, pp. 285–290.

[6] S. Padhye, N. Tiwari, Ecdlp-based certificateless proxy signature scheme with message recovery, Trans. Emerg. Telecommun. Technol. (2012) http://dx.doi.org/10.1002/ett.2608.

[7] H. Xiong, F. Li, Z. Qin, A provably secure proxy signature scheme in certificateless cryptography, Informatica 21 (2) (2010) 277–294.

[8] L. Zhang, F. Zhang, Q. Wu, Delegation of signing rights using certificateless proxy signatures, Inform. Sci. 184 (2012) 298–309.

[9] SK.-H. Islam, G.P. Biswas, Provable secure and pairing-free certificateless digital signature scheme using elliptic curve cryptography, Int. J. Comput. Math. 90 (11) (2013) 2244–2258.