Cryptanalysis of Provably Secure Certificateless Short Signature Scheme

Jayaprakash Kar

Information Security Research Group
Department of Information Systems
Faculty of Computing & Information Technology
King Abdulaziz University,
Kingdom of Saudi Arabia, Jeddah-21589
jgopabandhu@kau.edu.sa

Abstract. Recently, Choi *et* al. proposed certificateless short signature scheme in random oracle model and the author claims that it is provably secure. Certificateless Public Key Cryptography is a new paradigm, where it allows resolving the inherent key escrow and key management problem. Attack to certificateless signature scheme are of two types as Type-I where the adversary can replace the public key of the user and cannot able to retrieve the master secret key from Key Generator Center (KGC). In Type-II, the adversary can able to obtain the master secret key and cannot replace the public key of the user. In this paper we have proven that, the proposed scheme is not secure against Type-I adversary. To prove, we solve linear Diophantine equation and obtain the partial-private key of the user.

Keywords:Diophantine equation, Bilinear map, Digital signature, Certificateless signature

1 Introduction

In conventional Public Key Infrastructure (PKI), the public key of the user is validated by a trusted third party called Certificate Authorities (CA). The user's public key is validated by issuing a digital certificate that is associated with this public key and user's identity. This is economics in computational cost and storage. To resolve this problem, Shamir [1] introduced Identity Based Cryptography (IBC) in 1984 where the user selects his public key as his own choices a unique number like phone number, IP address, e-mail address etc. Further, the user could not generate his own private key as in conventional public key cryptography (PKC). Private Key of all users is generated and maintain by Key Generation Center (KGC). However there is key escrow problem. Since the private key can be misused always so that, ciphertext can be decrypted and forge the signature by any user. To eliminate the inherent key escrow problem of IBC and certificate management in traditional PKC, Al-Riyami and Paterson [2] introduced a new cryptographic paradigm in 2003 known as Certificateless Public Key Cryptography (CL-PKC). In CL-PKC, KGC constructs partial-private key for the user. Then the user chooses a secret value randomly and takes the partial-private key and generates the public key. In CL-PKC, public key of the user is transmitted along with the signature and the public key does not require the certification by the CA. Both the user's identity and public key are required for both for encryption and signature generation. Al-riyami and Paterson [2] suggested a novel technique in 2003 to resolve both the inherent key escrow problem of IBC and the use of certificates in conventional PKC. However the scheme has been proven that, it is insecure against Type-I adversary and by Huang *et* al. [3] proposed an improve version. After that numerous CLS [12, 5, 4] have been proposed in random oracle model. Subsequently the schemes are vulnerable to Type-I attack [8, 9, 4]. In 2006 Libert and Quisquater [11] proposed generic construction of CL-signature scheme without pre-computations. Gorantla and Saxena proposed a provably secure and efficient signature scheme [12] in 2005. However Cao *et* al. [13] proved that it vulnerable to Key Replacement Attack. Huang *et* al. [14] proposed two new short CLS schemes on random oracle model in 2007 and proved that, the first scheme is secure against both Normal Type-I adversary and Super Type-II adversary. Further claimed that the second scheme is secure against Super Type-I as well as super Type-II adversaries. However, the first scheme have been proven by Shim [15] that, it is universally forgeable byType-I adversary.

Recently Xu *et* al. in [16] proposed two CLS schemes which are suited to implement on mobile wireless cyber-physical systems, and emergency mobile wireless cyber-physical systems respectively and claim that the schemes are provably secure and efficient in computation. However, Zhang *et* al. [18, 17] proved that these two schemes are vulnerable to Public Key replacement attack and universally forgeable.

The paper is organized as follows. Section-2 presents some mathematical assumptions on bilinear pairings. In Section-3 we have reviewed Choi *et* al.'s scheme and section-4 describes the details of cryptanalysis of the scheme.

2 Mathematical Background

2.1 Bilinear Pairings

Let $\mathbb{G}_1$ be a cyclic additive group of prime order q and $\mathbb{G}_2$ be a cyclic multiplicative group of the same prime order q. Let $\hat{e}$ be a bilinear map which is non-degenerated and computable called admissible bilinear map if it satisfies the following properties:

$$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$$

holds following

- **Bilinearity**: Let $a, b \in \mathbb{Z}_q^*$ and $P, Q \in \mathbb{G}_1$
  1. $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ for all $a, b \in \mathbb{Z}_q^*$
  2. $\hat{e}(P + Q, R) = \hat{e}(P, R)\hat{e}(Q, R)$, for $P, Q, R \in \mathbb{G}_1$.
- **Non-degenerate**: There exists $P \in \mathbb{G}_1$ such that $\hat{e}(P, P) \neq 1_{\mathbb{G}_2}$
- **Computability**: There exist an efficient algorithm to compute $\hat{e}(P, Q)$ or all $P, Q \in \mathbb{G}_1$.

3 Review of Choi *et* al.'s CLS-Short Signature Scheme

In this section, we outline the provably secure certificateless short signature scheme proposed by Choi *et* al. [7]. It comprises the following six algorithms:

- `Setup`:
  1. Let $\mathbb{G}_1$ and $\mathbb{G}_2$ are two cyclic groups of prime order q. e is an admissible bilinear map.
  2. Choose $s \in \mathbb{Z}_q^*$ randomly and P of $\mathbb{G}_1$ be the generator. Compute $P_{pub} = sP$. s is the master secret key.
  3. $H_0, H_1, H_2 : \{0, 1\}^* \rightarrow \mathbb{G}^*$ and $H_3, H_4 : \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$, where $H_i, i = 0, 1, 2, 3, 4$ are collision resistant cryptographic hash function.
- `Partial-Private key Extract`: The algorithm takes `params`, master secret key s and identity ID of the user as input and returns partial-private key $D_{ID} = sQ_{ID} = sH_0(ID)$ and $D'_{ID} = sQ'_{ID} = sH_1(ID)$. Returns the user's partial-private key $SK_{ID} = <D_{ID}, D'_{ID}>$
- `Set-Secret-Value`: On input parameter k and user's identity ID, chooses $x_{ID} \in \mathbb{Z}_q^*$ randomly and returns a secret value x_{ID} of the user.
- `Set-Public key`: It takes input `params` and the secret value x_{ID} and computes $PK_{ID} = x_{ID}P$ and returns the user's public PK_{ID}.
- `Sign`: The algorithm takes the parameter `params`, ID, SK_{ID} and message to be sign m as input and performs the following steps:
  1. Set $T = H_2(m, PK_{ID}, ID)$, $h = H_3(m, PK_{ID}, ID)$ and $h' = H_4(m, PK_{ID}, ID)$
  2. Computes $\sigma = x_{ID}T + hD_{ID} + h'D'_{ID}$
  3. Return the signature σ for message m.
- `Verify`: On input `params`, ID, PK_{ID}, m and σ, the algorithm perform the following steps:
  1. Computes $Q_{ID} = H_0(ID)$, $Q'_{ID} = H_1(ID)$.
  2. Computes $T = H_2(m, PK_{ID}, ID)$, $h = H_3(m, PK_{ID}, ID)$ and $h' = H_4(m, PK_{ID}, ID)$
  3. Verify the equation $e(\sigma, P) = e(T, PK_{ID})e(hQ_{ID} + h'Q'_{ID}, P_{pub})$. If the equation holds, it returns 1, otherwise 0.

4 Cryptanalysis of Choi *e*t al.'s Scheme

The adversary $\mathcal{A}_I$ performs the following steps:

- Chooses a random number $\tilde{x}_{ID} \in \mathbb{Z}_q^*$ and replaces the user public key PK_{ID} with $\tilde{PK}_{ID} = \tilde{x}_{ID}P$.
- With respect to the security model defined in [], $\mathcal{A}_I$ submits query on `CL-Sign`. Since $\mathcal{A}_I$ is allowed to access signing oracle, he can replace a public key of his choice with the existing public key. Let the public key be $\tilde{PK}_{ID} = \tilde{x}_{ID}P$. Then computes a valid signature as

  $$\tilde{\sigma} = \tilde{x}_{ID}\tilde{T} + \tilde{h}D_{ID} + \tilde{h}'D'_{ID}$$

  Where $D_{ID} = sQ_{ID} = sH_0(ID)$ and $D'_{ID} = sQ'_{ID} = sH'_0(ID)$
- Finally $\mathcal{A}_I$ find the solution of the following linear Diophantine equation

  $$\tilde{h}D_{ID} + \tilde{h}'D'_{ID} = \mu \tag{1}$$

  Where $\mu = \tilde{\sigma} - \tilde{x}_{ID}\tilde{T}$ and $\mu \in \mathbb{Z}_q^*$. The equation has an integer solution in D_{ID} and $D'_{ID} \in \mathbb{Z}_q^* \iff gcd(\tilde{h}, \tilde{h}') \mid \mu$. Let we find a particular solution. By extended Euclidean algorithm, we compute the greatest common divisor gcd and such α_1 and α_2 that

  $$\tilde{h} \cdot \alpha_1 + \tilde{h}' \cdot \alpha_2 = gcd(\tilde{h}, \tilde{h}')$$

  Multiply $\tilde{h}''$ both sides we get

  $$\tilde{h} \cdot \alpha_1\tilde{h}'' + \tilde{h}' \cdot \alpha_2\tilde{h}'' = gcd(\tilde{h}, \tilde{h}')\tilde{h}''.$$
  $$\Rightarrow \tilde{h}\frac{\alpha_1 \cdot \tilde{h}''}{gcd(\tilde{h}, \tilde{h}')} + \tilde{h}'\frac{\alpha_2 \cdot \tilde{h}''}{gcd(\tilde{h}, \tilde{h}')} = \mu.$$

  Compare this with the original equation-1, it follows that the particular equation is

  $$D_{ID} = \frac{\tilde{h}\mu}{gcd(\tilde{h}, \tilde{h}')} \text{ and } D'_{ID} = \frac{\tilde{h}'\mu}{gcd(\tilde{h}, \tilde{h}')}$$

Hence the scheme proposed by Choi *e*t al. is insecure against `Type-I` adversary where he can able to replace the user's public key and construct a valid forge of the signature for any message after accessing the signing oracle.

5 Conclusion

Recently Choi *e*t al. proposed CLS-Signcryption scheme and claimed that their scheme is secure against the super adversary. However we analyze and review the scheme and scheme and prove that the scheme is vulnerable to `Type-I` attack, where the adversary $\mathcal{A}_I$ can access the signing oracle and can replace his chosen public key and make a valid forge signature.

6 Acknowledgments

The author would like to thank to Deanship of Scientific Research(DSR), King Abdulaziz University, P.O.Box-80221, Jeddah-21589, Kingdom of Saudi Arabia for their technical and financial support. This work is supported by DSR under Distinct Study Research, grant No. `611-34-D1435`.

References

1. A. Shamir "Identity-based cryptosystems and signature schemes", *in Advances in Cryptology, vol. 196 of Lecture Notes in Computer Science*, pp. 47–53, Springer, Berlin, Germany, 1984.
2. S. S. Al-Riyami and K. G. Paterson "Certificateless public key cryptography",*in Advances in Cryptology-ASIACRYPT 2003,vol. 2894 of Lecture Notes in Computer Science*, pp. 452–473, Springer, Berlin, Germany, 2003.
3. X. Huang, W. Susilo, Y. Mu, and F. Zhang "On the security of certificateless signature schemes from ASIACRYPT 2003", *in Cryptology and Network Security, vol. 3810 of Lecture Notes in Computer Science*, pp. 13–25, Springer, Berlin, Germany, 2005.

4. X. Li, K. Chen, L. Sun "Certificateless signature and proxy signature schemes from bilinear pairings", *Lithuanian Mathematical Journal* 45(1), pp.76–83, 2005.
5. W.S. Yap, S.H. Heng, B.M. Goi "An efficient certificateless signature scheme, emerging directions in embedded and ubiquitous computing",*in EUC Workshops 2006, LNCS, vol. 4097, Springer-Verlag*, pp. 322–331, 2006.
6. M.C. Gorantla, A. Saxena "An efficient certificateless signature scheme", *in CIS05, LNAI, vol. 3802, Springer-Verlag*, pp. 110–116, 2005.
7. K. Y. Choi, J. H. Park, and D. H. Lee "A new provably secure certificateless short signature scheme",*Computers and Mathematics with Applications*, vol. 61,no.7, pp. 1760–1768, 2011.
8. Z. Zhang, D. Feng Key replacement attack on a certificateless signature scheme, Cryptology ePrint Archive: Report 2006/453.
9. M.H. Au, J. Chen, J.K. Liu, Y. Mu, D.S. Wong, G. Yang " Malicious KGC attacks in certificateless cryptography", *in: ASIACCS07, ACM*, pp. 302311, 2007. available at Cryptology ePrint Archive: Report 2006/255.
10. X. Cao, K.G. Paterson, W. Kou An attack on a certificateless signature scheme, Cryptology ePrint Archive: Report 2006/367.
11. B. Libert and J. J. Quisquater "On constructing certificateless cryptosystems from identity based encryption", *in Proceedings of the 9th International Conference on Theory and Practice of Public-Key Cryptography (PKC 06), vol. 3958 of Lecture Notes in Computer Science*, pp. 474–490, Springer, Berlin, Germany, 2006.
12. M.Gorantla and A. Saxena "An efficient certificateless signature scheme", *in Computational Intelligence and Security, vol. 3802 of Lecture Notes in Computer Science*, pp. 110–116, Springer, Berlin, Germany, 2005.
13. X. Cao, K. G. Paterson, and W. Kou "An attack on a certificateless signature scheme", *Cryptology EPrint Archive 2006/367, 2006, http://eprint.iacr.org.*
14. X. Huang, Y.Mu, W. Susilo, D. S.Wong, and W.Wu "Certificateless signature revisited in Information Security and Privacy", vol. 4586 of Lecture Notes in Computer Science, pp. 308322, Springer, Berlin, Germany, 2007.
15. K. Shim "Breaking the short certificateless signature scheme",*Information Sciences*, vol. 179, no. 3, pp. 303306, 2009.
16. Z. Xu, X. Liu, G. Zhang, W. He, G. Dai, and W. Shu "A certificateless signature scheme for mobile wireless cyber-physical systems", *in 28th International Conference on Distributed Computing Systems Workshops, ICDCS Workshops 2008, pp. 489–494, June 2008.*
17. Z. Xu, X. Liu, G. Zhang, and W. He "McCLS: certificateless signature scheme for emergency-mobile wireless cyber-physical systems", *International Journal of Computers, Communications and Control*, vol. 3, no. 4, pp. 395–411, 2008.
18. F.Zhang, S.Miao, S. Li,Y.Mu,W. Susilo, and X. Huang "Cryptanalysis on two certificateless signature schemes", *International Journal of Computers, Communications and Control*, vol. 5, no. 4, pp. 586–591, 2010.