ICIC Express Letters
Volume **11**, Number **3**, March **2017**
 ISSN 1881-803X
pp. **619–624**

CRYPTANALYSIS OF PROVABLY SECURE CERTIFICATELESS SHORT SIGNATURE SCHEME BY SOLVING LINEAR DIOPHANTINE EQUATIONS

Jayaprakash Kar

Department of Computer Science and Engineering
The LNM Institute of Information Technology
Rupa ki Nangal, Post-Sumel, Via-Jamdoli Jaipur-302031, Rajasthan, India
jayaprakashkar@lnmiit.ac.in

Received May 2016; accepted August 2016

Abstract. *Recently, Choi et al. proposed certificateless short signature scheme in random oracle model and the authors claim that it is provably secure. Attacks to certificateless signature scheme are of two types as* `Type-I` *and* `Type-II`*. In* `Type-I`*, the adversary can replace the public key of the user and cannot be able to retrieve the master secret key from key generator center (KGC) whereas in* `Type-II`*, the adversary can be able to obtain the master secret key and cannot replace the public key of the user. However, cryptanalysis and vulnerability are shown by Chen et al. However, in this paper, we prove the scheme is vulnerable to* `Type-I` *attack in a simpler way by solving 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, and e-mail address. 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 maintained by key generation center (KGC). However, there is key escrow problem. Since the private key can be misused always, 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 [3] 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 encryption and signature generation.

Certificateless public key cryptography is a new paradigm, where it allows to resolve the inherent key escrow and key management problem. Al-Riyami and Paterson [3] 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 Huang et al. [4] proposed an improved version. After that numerous CLS [5, 6, 13] have been proposed in random oracle model. Subsequently the schemes are vulnerable to `Type-I` attack [5, 9, 10]. In 2006 Libert

and Quisquater [12] proposed generic construction of CL-signature scheme without pre-computations. Gorantla and Saxena proposed a provably secure and efficient signature scheme [13] in 2005. However, Cao et al. [14] proved that it is vulnerable to key replacement attack. Huang et al. [15] 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 claim that the second scheme is secure against super `Type-I` as well as super `Type-II` adversaries. However, the first scheme has been proven by Shim [16] that, it is universally forgeable by `Type-I` adversary.

Recently, Xu et al. in [17] 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, 19] proved that these two schemes are vulnerable to public key replacement attack and universally forgeable. In 2013, Chen et al. showed the cryptanalysis and vulnerability of Choi et al.'s CLS scheme [2] and prove that the scheme is not secure against strong `Type-I` attack. However, the attacker needs to perform costly inverse operation of the hash function to obtain the partial private key.

The paper is organized as follows. Section 2 presents some mathematical assumptions on bilinear pairings. Section 3 describes the framework of certificateless signature scheme, and in Section 4, the security model is illustrated. In Section 5, we have reviewed Choi et al.'s scheme and Section 6 describes the details of cryptanalysis of Choi et al.'s scheme. Finally, this paper concludes in Section 7.

2. **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:

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

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 exists an efficient algorithm to compute $\hat{e}(P, Q)$ or all $P, Q \in \mathbb{G}_1$.

3. **Certificateless Signature Scheme.** A CLS signature scheme comprises six polynomialy solvable algorithms.

- `Setup`: The algorithm takes the security parameter λ as input and returns the system parameter `params` and master secret key.
- `Partial-Private-Key-Extract`: This algorithm takes the system parameter `params`, master secret key and the user's identity ID and returns partial private key d_{ID} corresponding to the identity ID for the user.
- `Set-Secret-Value`: This algorithm takes the security parameter λ, user's identity ID and returns a secret value x_{ID} corresponding to the user with identity ID.
- `Set-Public-Key`: This algorithm takes the secret value x_{ID} of the user as input and returns the public key pk_{ID} corresponding to the user with identity ID.
- `CL-Sign`: This algorithm takes system parameter `params`, a message m and user's private key sk_{ID} as input and returns the signature σ.
- `CL-Verify`: This algorithm takes the system parameter `params`, message m, public key pk_{ID}, user's identity ID and signature σ as input and returns either 1 if the signature is valid, otherwise returns 0.

4. **Security Model.** Security model of CLS signature scheme is defined by the game between the adversary and challenger. There are two types of adversaries defined as:

- `Type-I` adversary ($\mathcal{A}_I$): The adversary acts as common dishonest user of the system and is not in possession of master secret key of KGC and he can replace a value for the user's public key of his own choice in an adaptive manner;
- `Type-II` adversary ($\mathcal{A}_{II}$): The adversary acts as honest user but is curious and does have access master secret key, but cannot replace user's public key.

The capabilities of these adversary are modeled by queries as a game played between the adversary and a challenger where they interact with each other and evaluate the chance of success to attack the system.

Game-1

`Initial`: The challenger $\mathcal{C}$ takes the security parameter λ, runs the algorithm `Setup` and returns the system parameter and master secret key. The challenger keeps master secret key secret.

The adversary $\mathcal{A}_I$ performs the following oracle queries in an adaptive manner and can request the hash value for any input. The number of queries submitted is polynomial bounded.

- `Extract partial private key`: $\mathcal{A}_I$ can ask the value for the partial private key, say d_{ID} for any input identity ID except the challenged identity ID. $\mathcal{C}$ runs the extraction of partial private key algorithm taking the input ID, master secret key and system parameter and computes the partial private key d_{ID} corresponding to the identity ID and returns d_{ID} to $\mathcal{A}_I$.
- `Extract private key`: $\mathcal{C}$ runs the extraction of private key and computes private key, say sk_{ID} for any identity ID except the challenged identity and returns sk_{ID} to $\mathcal{A}_I$.
- `Request public key`: $\mathcal{A}_I$ chooses an identity ID submitting the queries for public key for the identity ID, and $\mathcal{C}$ computes the corresponding public key pk_{ID} and returns to $\mathcal{A}_I$.
- `Replace public key`: For any identity ID, $\mathcal{A}_I$ chooses a secret value of his own choice and computes the new public key. Then it replaces the value for public key with the current one pk_{ID}.
- `CL-Sign queries`: The oracle takes the user's identity ID and the message m to be signed, and $\mathcal{C}$ generates the signature σ using his private key sk_{ID} corresponding to the identity ID and sends to $\mathcal{A}_I$. The oracle checks the condition of whether the public key pk_{ID} has been replaced by $\mathcal{A}_I$ or not. If it is replaced, then $\mathcal{C}$ cannot find pk_{ID} and the answer of signing oracle might be incorrect. Here, $\mathcal{A}_I$ queries the secret value $\tilde{x}_{ID}$ additionally corresponding to the replaced public key pk_{ID} to the signing oracles.

  Finally, $\mathcal{A}_I$ returns a signature σ^* on message m^* corresponding to the public key pk^*_{ID} for challenged user's identity ID^*. If all the parameters pass through the verification, i.e., `CL-Verify` (`params`, ID^*, m^*, pk^*_{ID}) $= 1$ then $\mathcal{A}_I$ wins the game with the following conditions.

  1) The queries for extraction of private key for the identity ID^* has never been submitted.
  2) The identity ID^* is not submitted to the oracle for which the public key is replaced as well as the private key is being extracted.
  3) Message m^*, public key pk^*_{ID} corresponding to the identity ID^* are not being never submitted to the signing oracle.

Game-2

This game is modeled by the following oracles where `Type-II` attacker interacts with the challenger and tries to win the game.

- `Initialize`: The challenger $\mathcal{C}$ takes the security parameter λ, runs the algorithm `Setup` and returns the system parameter and master secret key. The adversary $\mathcal{A}$ is allowed to access the master secret key which is to be sent by the challenger.
- `Extract Private key`: $\mathcal{C}$ runs the extraction of private key and computes private key, say sk_{ID} for any identity ID except the challenged identity and returns sk_{ID} to $\mathcal{A}_{II}$.
- `Request Public key`: $\mathcal{A}_I$ chooses an identity ID submitting the queries for public key for the identity ID, and $\mathcal{C}$ computes the corresponding public key pk_{ID} and returns to $\mathcal{A}_{II}$.
- `CL-Sign Queries`: The oracle takes the user's identity ID and the message m to be signed, and $\mathcal{C}$ generates the signature σ using his private key sk_{ID} corresponding to the identity ID and sends to $\mathcal{A}_{II}$.

  Finally, $\mathcal{A}_{II}$ returns a signature σ^* on message m^* corresponding to the public key pk^*_{ID} for challenged user's identity ID^*. $\mathcal{A}_I$ wins the game with the following conditions:
  1) If all the parameters pass through the verification, i.e., `CL-Verify` (`params`, ID^*, m^*, pk^*_{ID}) $= 1$.
  2) Message m^*, public key pk^*_{ID} corresponding to the identity ID^* are not being never submitted to the signing oracle.

Definition 4.1. *A CLS signature scheme is said to be existentially unforgeable against adaptive chosen message attacks, if the probability of success of attacker $\mathcal{A}_I$ and $\mathcal{A}_{II}$ in the above two games are negligible.*

5. **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. [8]. It comprises the following six algorithms.

- `Setup`:
  1) Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic groups of prime order q. e is an admissible bilinear map.
  2) Choose $s \in \mathbb{Z}_q^*$ randomly and P of $\mathbb{G}_1$ is the generator. Compute $P_{pub} = sP$. s is the master secret key.
  3) $H_0, H_1, H_2 : \{0,1\}^* \to \mathbb{G}^*$ and $H_3, H_4 : \{0,1\}^* \to \mathbb{Z}_q^*$, 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 $D'_{ID} = sQ'_{ID} = sH_1(ID)$. Return the user's partial-private key $SK_{ID} = <D_{ID}, D'_{ID}>$.
- `Set-Secret-Value`: On input parameter k and user's identity ID, choose $x_{ID} \in \mathbb{Z}_q^*$ randomly and return 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 return 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) Compute $\sigma = x_{ID}T + hD_{ID} + h'D'_{ID}$
  3) Return the signature σ for message m.
- `Verify`: On input `params`, ID, PK_{ID}, m and σ, the algorithm performs the following steps:
  1) Compute $Q_{ID} = H_0(ID)$, $Q'_{ID} = H_1(ID)$.
  2) Compute $T = H_2(m, PK_{ID}, ID)$, $h = H_3(m, PK_{ID}, ID)$ 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.

6. **Cryptanalysis of Choi et al.'s Scheme.** The adversary $\mathcal{A}_I$ performs the following steps.

- Choose a random number $\tilde{x}_{ID} \in \mathbb{Z}_q^*$ and replace the user public key PK_{ID} with $\widetilde{PK}_{ID} = \tilde{x}_{ID}P$.
- With respect to the security model defined in [6], $\mathcal{A}_I$ submits query on `CL-Sign`. Since $\mathcal{A}_I$ is allowed to access signing oracle, it can replace a public key of its choice with the existing public key. Let the public key be $\widetilde{PK}_{ID} = \tilde{x}_{ID}P$. Then compute a valid signature as
$$\tilde{\sigma} = \tilde{x}_{ID}\widetilde{T} + \tilde{h}D_{ID} + \tilde{h}'D'_{ID}$$
where $D_{ID} = sQ_{ID} = sH_0(ID)$ and $D'_{ID} = sQ'_{ID} = sH'_0(ID)$
- Finally, $\mathcal{A}_I$ finds 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 $D'_{ID} \in \mathbb{Z}_q^* \iff gcd\left(\tilde{h}, \tilde{h}'\right) \Big| \mu$. Let us find a particular solution. By extended Euclidean algorithm, we compute the greatest common divisor gcd and such α_1 and α_2 that
$$\tilde{h} \cdot \alpha_1 + \tilde{h}' \cdot \alpha_2 = gcd\left(\tilde{h}, \tilde{h}'\right)$$
Multipling $\tilde{h}''$ both sides we get
$$\tilde{h} \cdot \alpha_1\tilde{h}'' + \tilde{h}' \cdot \alpha_2\tilde{h}'' = gcd\left(\tilde{h}, \tilde{h}'\right)\tilde{h}''$$
$$\Rightarrow \tilde{h}\frac{\alpha_1 \cdot \tilde{h}''}{gcd\left(\tilde{h}, \tilde{h}'\right)} + \tilde{h}'\frac{\alpha_2 \cdot \tilde{h}''}{gcd\left(\tilde{h}, \tilde{h}'\right)} = \mu$$
Compare this with the original Equation (1), it follows that the particular equation is
$$D_{ID} = \frac{\tilde{h}\mu}{gcd\left(\tilde{h}, \tilde{h}'\right)} \text{ and } D'_{ID} = \frac{\tilde{h}'\mu}{gcd\left(\tilde{h}, \tilde{h}'\right)}$$

Hence the scheme proposed by Choi et al. is insecure against `Type-I` adversary where it can be able to replace the user's public key and construct a valid forge of the signature for any message after accessing the signing oracle.

7. **Conclusion.** Recently, Choi et al. proposed CLS-signcryption scheme and claimed that their scheme is secure against the super adversary. However, we analyze and review the 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 its chosen public key and make a valid forge signature. Our technique is more efficient than Chen et al.'s technique where the attacker needs to perform costly inverse operation of the hash function to obtain the partial private key.

REFERENCES

[1] A. Shamir, Identity-based cryptosystems and signature schemes, *Advances in Cryptology, Volume 196 of the Book Series Lecture Notes in Computer Science*, pp.47-53, 1984.

[2] Y.-C. Chen, R. Tso and G. Horng, Cryptanalyis of a provably secure certificateless short signature scheme, *Intelligence Systems & Applications*, pp.61-68, 2013.

[3] S. S. Al-Riyami and K. G. Paterson, Certificateless public key cryptography, *Advances in Cryptology, Volume 2894 of the Book Series Lecture Notes in Computer Science*, pp.452-473, 2003.

[4] X. Huang, W. Susilo, Y. Mu and F. Zhang, On the security of certificateless signature schemes from Asiacrypt 2003, *Cryptology and Network Security, Volume 3810 of the Book Series Lecture Notes in Computer Science*, pp.13-25, 2005.

[5] X. Li, K. Chen and L. Sun, Certificateless signature and proxy signature schemes from bilinear pairings, *Lithuanian Mathematical Journal*, vol.45, no.1, pp.76-83, 2005.

[6] W. S. Yap, S. H. Heng and B. M. Goi, An efficient certificateless signature scheme, emerging directions in embedded and ubiquitous computing, *EUC Workshops 2006, LNCS*, vol.4097, pp.322-331, 2006.

[7] M. C. Gorantla and A. Saxena, An efficient certificateless signature scheme, *Computational Intelligence and Security, Volume 3802 of the Series Lecture Notes in Computer Science*, pp.110-116, 2005.

[8] 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.

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

[10] M. H. Au, J. Chen, J. K. Liu, Y. Mu, D. S. Wong and G. Yang, Malicious KGC attacks in certificateless cryptography, *Proc. of ASIACCS, Cryptology ePrint Archive: Report 2006/255*, Singapore, pp.302-311, 2007.

[11] X. Cao, K. G. Paterson and W. Kou, An attack on a certificateless signature scheme, *Cryptology ePrint Archive: Report 2006/367*, 2006.

[12] B. Libert and J. J. Quisquater, On constructing certificateless cryptosystems from identity based encryption, *Proc. of the 9th International Conference on Theory and Practice of Public-Key Cryptography, Volume 3958 of the Series Lecture Notes in Computer Science*, pp.474-490, 2006.

[13] M. Gorantla and A. Saxena, An efficient certificateless signature scheme, *Computational Intelligence and Security, Volume 3802 of the Series Lecture Notes in Computer Science*, pp.110-116, 2005.

[14] X. Cao, K. G. Paterson and W. Kou, An attack on a certificateless signature scheme, *Cryptology EPrint Archive 2006/367*, http://eprint.iacr.org, 2006.

[15] X. Huang, Y. Mu, W. Susilo, D. S. Wong and W. Wu, Certificateless signature revisited, *Information Security and Privacy, Volume 4586 of the Series Lecture Notes in Computer Science*, pp.308-322, 2007.

[16] K. Shim, Breaking the short certificateless signature scheme, *Information Sciences*, vol.179, no.3, pp.303-306, 2009.

[17] Z. Xu, X. Liu, G. Zhang, W. He, G. Dai and W. Shu, A certificateless signature scheme for mobile wireless cyber-physical systems, *The 28th International Conference on Distributed Computing Systems Workshops*, pp.489-494, 2008.

[18] Z. Xu, X. Liu, G. Zhang and W. He, McCLS: Certificateless signature scheme for emergencymobile wireless cyber-physical systems, *International Journal of Computers, Communications and Control*, vol.3, no.4, pp.395-411, 2008.

[19] 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.