Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 102508, 6 pages
http://dx.doi.org/10.1155/2013/102508

Research Article

On the Security of Certificateless Signature Schemes

Gaurav Sharma, Suman Bala, and Anil K. Verma

Computer Science and Engineering Department, Thapar University, Patiala 147004, India

Correspondence should be addressed to Gaurav Sharma; gaurav.sharma@thapar.edu

Received 21 December 2012; Revised 19 May 2013; Accepted 20 May 2013

Academic Editor: J. Barbancho

Wireless Sensor Network (WSN) has proved its presence in various real time applications and hence the security of such embedded devices is a vital issue. Certificateless cryptography is one of the recent paradigms to provide security. Certificateless public key cryptography (CL-PKC) deals effectively with the twin issues of certificate management in traditional public key cryptography and key escrow problem in identity-based cryptography. CL-PKC has attracted special attention in the field of information security as it has opened new avenues for improvement in the present security architecture. Recently, Tsai et al. proposed an improved certificateless signature scheme without pairing and claimed that their new construction is secure against different kinds of attacks. In this paper, we present a security analysis of their scheme and our results show that scheme does not have resistance against malicious-KGC attack. In addition, we have found some security flaws in the certificateless signature scheme of Fan et al. and proved the scheme vulnerable to Strong Type I attack.

1. Introduction

The validation of public keys by a trusted third party, also known as Certificate Authority (CA), makes traditional Public Key Infrastructure (PKI) uneconomical. The user selects a public key and then CA provides a digital certificate to associate the public key with the user's identity. The management of these certificates is a complex issue and increases the computation and storage cost manifold. To resolve the issues of PKC a revolutionary ID-based infrastructure was introduced by Shamir [1] in 1984. This seminal concept of Identity Based Cryptography (IBC) allows the user to choose a public key of its own choice such as email ID, phone number, and name. In IBC, users do not generate their own private keys as in traditional PKC. Private keys are generated by Key Generation Centre (KGC), maintains the private keys of all the users, but there is always a possibility of the misuse of these private keys as they can be used to decrypt any ciphertext and forge the signature of user on any message for signature generation. Eventually, this new paradigm solved the problem of certificate management but gave birth to inherent problem of key escrow.

In 2003, Al-riyami and Paterson [2] proposed a novel approach to eliminate the inherent key escrow problem of IBC as well as the use of certificates in traditional PKC. This approach is known as CL-PKC, where KGC generates a partial-private key for the user while user's secret key and partial-private key are used to generate the public key of the user. In other words, CL-PKC differs from IBC in terms of arbitrary public key, and when a signature is transmitted, user's public key is attached with it but not certified by any of the trusted authority. Moreover, KGC is not aware of the secret key of the user.

However, Al-riyami and Paterson's [2] scheme has been proved insecure against Type I adversary by Huang et al. [3] and proposed an improved scheme. A generic construction has been proposed by Yum and Lee [4] in 2004 which is based on identity based signature. Later, Hu et al. [5] found it insecure against key replacement attack and proposed an improved version. Meanwhile Libert and Quisquater [6] proposed another generic construction without precomputations, which is based on Al-riyami and Paterson's work. In 2005, Gorantla and Saxena [7] proposed an efficient CLS scheme but it was found to be insecure against the key replacement attack by Cao et al. [8]. Li et al. [9] and Zhang et al. [10] proposed CLS schemes based on elliptic curve but verification algorithms in their schemes require four pairing computations. To improve the performance, Yap et al. [11] proposed an efficient CLS scheme which required only two bilinear pairings. However, Park and Kang [12] found that

the scheme [11] is insecure against a key replacement attack. Recently, Au et al. [13] suggested a new kind of malicious-but-passive-KGC attack where adversary may get access to the secret/public key of KGC and then modified Hu et al.'s model [5] for capturing the attack. In 2007, Huang et al. [14] proposed two new short CLS schemes and claimed their first scheme is provably secure against a Normal Type I adversary as well as Super Type II adversary and the second scheme is secure against Super Type I and Type II adversaries. Unfortunately, Shim [15] claimed that the first scheme in [14] is universally forgeable by the Type I adversary. Later, Tso et al. [16–18] presented efficient short CLS schemes. Recently two CLS schemes were proposed by Xu et al. in [19, 20] for mobile wireless cyber-physical systems, and emergency mobile wireless cyber-physical systems respectively. They were claimed to provide high efficiency and provable security. However, Zhang et al. [21] has shown that these two schemes are universally forgeable against public key replacement attack. Wang et al. [22] proposed a scheme which need not compute the pairing $e(P, P) = g$ at the sign stage, rather it precomputes and publishes the system parameters.

Recently, Du and Wen [23] presented a short CLS scheme and claimed that it is secure against Strong adversaries. However, Fan et al. [24] and Choi et al. [25] independently showed it to be insecure against Strong Type I adversary. Further, Fan et al. [24] proposed a CLS scheme from bilinear pairing with additional property of nonrepudiation but later it was found in [26] that the scheme does not acheive Girault's level 3 security. Later, Tian et al. [27] claimed that the scheme [25] didnot withstand against Strong Type II adversary.

In certificateless infrastructure, the majority of the schemes lacks in some common security issue. To attack a CLS scheme broadly two types of adversaries have been defined: Type I and Type II. A Type I adversary can replace a user's public key but is not able to obtain KGC's master secret key and a Type II adversary is a malicious KGC who knows the master secret key but cannot replace user's public key. Although Huang et al. [28] divide the potential adversaries according to their attack power and enrich the CL-PKC with three more categories. A clear definition of all the three categories of adversaries, Normal, Strong, and Super, has been provided together with the security models. On association with the existing categorization of Type I and Type II adversaries, six types of adversaries can be obtained. These are Normal Type I, Strong Type I, Super Type I, Normal Type II, Strong Type II, and Super Type II. In fact, if a scheme is secure against a Super Type I (II) adversary, it will guarantee the security against Normal and Strong Type I (II) adversaries but the reverse may not be true.

In any certificateless scheme, it is always a good idea to avoid pairing operation as it leads to the increase in computation cost manifold as compared to any other operation. An interesting attempt has been made by He et al. [29] in 2011. He et al. developed an efficient short CLS scheme without pairing. The advantage of the scheme is that it does not use any pairing operation and the length of signature is short. However, in 2012, Tian and Huang [30] proved that the scheme cannot resist against Strong Type II adversary having an access to the master secret key of the KGC. Later Tsai et al. [31] discovered that the short CLS scheme [29] cannot withstand against Type II adversary and proposed an improved scheme to overcome the weaknesses of He et al.'s [29] scheme. In this paper, we provide a cryptanalysis on the Tsai et al. [31] scheme by using two Type II attacks.

As all the schemes based on ID-based cryptography have been implemented on sensor network, so these schemes are similarly applicable to Wireless Sensor Network [32]. Mica2, Micaz, Tmote sky, and TelosB are the commonly available motes and can be used for implementation. Evaluation of these schemes can be on the basis of various factors like energy consumption, computation time, and security provided. The schemes discussed here in this papers are very much of interest because they are free from pairing, so easily applicable to WSN. But with less resource consumption scheme should not compromise with security. These schemes are found to be vulnerable and few flaws have been reported. In this paper few attacks have been given which will help to improve the scheme.

The rest of the paper is organized as follows. Section 2 presents some preliminaries and complexity assumptions. Section 3 reviews the Tsai et al.'s scheme [31]. In Section 4, we discuss the security analysis of Tsai et al.'s scheme and prove that the scheme is insecure against Strong Type II attack. Section 5 reviews the Fan et al.'s scheme [24]. In Section 6, we discuss the security analysis of Fan et al.'s scheme and proved in insecure against Strong Type I attack followed by the concluding remarks on the presented work.

2. Preliminaries

This section revisits the fundamentals used in the CLS scheme.

2.1. Overview of Elliptic Curve Cryptography. An elliptic curve [33, 34] is a set of points over a finite field $GF(p)$, a Galois Field of order p, which satisfies the Weierstra $\mathscr{B}$ equation [35]

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

but for simplification of computations, cryptographic applications prefer the simple form of Weierstra $\mathscr{B}$ equation as

$$y^2 = x^3 + ax + b, \tag{2}$$

where $a, b \in GF(p)$.

2.2. Complexity Assumptions. The security of elliptic curve based cryptosystem is based on the assumption that the Elliptic Curve Discrete Logarithm Problem (ECDLP) is hard, which can be defined as follows.

Let E be an elliptic curve over a finite field F_p. Suppose, there are points P, Q on the curve $E(F_p)$ for given generator P. Determine k such that $Q = [k]P$.

3. Review of Tsai et al.'s Short CLS Scheme

In this section, we briefly review the short certificateless signature scheme based on ECDLP [31]. The scheme works as follows.

Setup. Let G be a cyclic additive group, let E/F_p be an elliptic curve E over a prime finite field F_p defined by an equation $y^2 = x^3 + ax + b$, and let p be k-bit prime number, where $p \in G$. Initially, the KGC computes its master public key $P_{\text{pub}} = xP$ and chooses two secure one-way hash functions: $H_1 : \{0,1\}^* \times G \times G \rightarrow Z_n^*$ and $H_2 : \{0,1\}^* \times G \times G \times G \rightarrow Z_n^*$, where $x \in Z_n^*$ is the master key chosen by KGC. The KGC then publishes public parameters $\{F_p, E/F_p, G, P, P_{\text{pub}}, H_1, H_2\}$ and keeps master key x secret.

Set-Secret Value. A signer chooses his/her identity ID and his/her secret value x_{ID}. The signer then computes $P_{\text{ID}} = x_{\text{ID}}P$ and keeps master key x secret x_{ID}.

Partial-Private-Key Extract. The KGC computes $R_{\text{ID}} = r_{\text{ID}}P$ and $h_{\text{ID}} = H_1(\text{ID}, R_{\text{ID}}, P_{\text{ID}})$ for each signer with his/her identity $\text{ID} \in \{0,1\}^*$, where $r_{\text{ID}} \in Z_n^*$ is a random number. The KGC then computes $s_{\text{ID}} = r_{\text{ID}} + h_{\text{ID}}x \bmod n$ and sends $(s_{\text{ID}}, R_{\text{ID}})$ to the user via a secure channel. Notably, the tuple $(s_{\text{ID}}, R_{\text{ID}})$ is the partial-private key of the user and the user can confirm its validity by checking the following equation: $s_{\text{ID}}P = R_{\text{ID}} + h_{\text{ID}} \cdot P_{\text{pub}}$. If the equation holds, the partial-private key $(s_{\text{ID}}, R_{\text{ID}})$ is valid; otherwise, the signer rejects the partial-private key $(s_{\text{ID}}, R_{\text{ID}})$.

Set-Private Key. The signer uses $sk_{\text{ID}} = (x_{\text{ID}}, s_{\text{ID}})$ as his/her private key.

Set-Public Key. The signer adopts $pk_{\text{ID}} = (P_{\text{ID}}, R_{\text{ID}})$ as his/her public key.

Sign. Assume a signer wants to sign a message m, he/she performs the following steps to generate signature (R, s) on chosen message m.

(i) The signer computes $R = l \cdot P$, $h_1 = H_2(m, R, P_{\text{ID}}, R_{\text{ID}})$, $h_2 = H_2(m, R, P_{\text{ID}}, R_{\text{ID}}, P_{\text{pub}})$, where r_{ID} is a random number.

(ii) The signer checks whether $gcd(l + h_1, n)$ equals 1. If it does not hold, the signer returns to step (i).

(iii) The signer computes $s = (l + h_1)^{-1}(h_2 \cdot x_{\text{ID}} + s_{\text{ID}}) \bmod n$ and then sends (R, s) to the verifier.

Verify. Upon receiving the signature (R, s) on message m from the signer, the verifier can confirm the validity of signature (R, s) using the following equation:

$$s \cdot (R + h_1 \cdot P) = h_2 \cdot P_{\text{ID}} + R_{\text{ID}} + h_{\text{ID}} \cdot P_{\text{pub}}, \tag{3}$$

where $h_1 = H_2(m, R, P_{\text{ID}}, R_{\text{ID}})$, $h_2 = H_2(m, R, P_{\text{ID}}, R_{\text{ID}}, P_{\text{pub}})$, and $h_{\text{ID}} = H_1(\text{ID}, R_{\text{ID}}, P_{\text{ID}})$.

If the above equation holds, signature (R, s) is valid; otherwise, the verifier rejects the signature.

4. Cryptanalysis of Tsai et al.'s Short CLS Scheme

In this section, we prove that the He et al. [29] CLS scheme is forgeable by the Strong Type II adversary; that is, the adversary can forge users certificateless signatures by using malicious-KGC attack. Tsai et al. proposed an improvement in the He et al.'s [29] scheme and claimed that the scheme is secure under discrete logarithm assumption in random oracle model. Unfortunately, the scheme was found to be insecure against the malicious-KGC attack.

4.1. Attack 1. The adversary $\mathcal{A}_{\text{II}}$ will perform the following steps.

(i) The adversary $\mathcal{A}_{\text{II}}$ choose random numbers $t, l' \in Z_n^*$ and a message m' and computes

$$R' = l'P. \tag{4}$$

The adversary $\mathcal{A}_{\text{II}}$ replaces the KGC's master public key P_{pub} with

$$P'_{\text{pub}} = \frac{t - R_{\text{ID}}}{h'_{\text{ID}}}, \tag{5}$$

where, $h'_{\text{ID}} = H_1(\text{ID}, P_{\text{ID}}, R_{\text{ID}})$.

And, the adversary generates the signature as

$$s' = \frac{t + h'_2 P_{\text{ID}}}{(l' + h'_1)P} \bmod n, \tag{6}$$

where $h'_1 = H_2(m', R', P_{\text{ID}}, R_{\text{ID}})$, $h'_2 = H_2(m', R', P_{\text{ID}}, R_{\text{ID}}, P'_{\text{pub}})$. Clearly, (R', s') is the forged signature on the message m'.

(ii) To check the validity of the signature, the verifier can perform the following verification by using the following equation:

$$\begin{aligned} s' \cdot \left(R' + h'_1 \cdot P\right) &= \frac{t + h'_2 P_{\text{ID}}}{(l' + h'_1)P} \cdot \left(l'P + h'_1 P\right) \\ &= t + h'_2 P_{\text{ID}} \\ &= h'_2 \cdot P_{\text{ID}} + \left[\frac{t - R_{\text{ID}}}{h'_{\text{ID}}} \cdot h'_{\text{ID}} + R_{\text{ID}}\right] \\ &= h'_2 \cdot P_{\text{ID}} + R_{\text{ID}} + h'_{\text{ID}} \cdot P'_{\text{pub}}. \end{aligned} \tag{7}$$

4.2. Attack 2. The adversary $\mathcal{A}_{\text{II}}$ will perform the following steps to forge a signature.

(i) The adversary $\mathcal{A}_{\text{II}}$ selects a random number $t' \in Z_n^*$ and computes $R' = t' \cdot P$.

(ii) $\mathcal{A}_{\text{II}}$ chooses a random number $r'_{\text{ID}} \in Z_n^*$ and computes $R'_{\text{ID}} = r'_{\text{ID}} \cdot P$.

(iii) The adversary obtains the hash values $h_1' = H_2(m', R', P_{ID}, R_{ID}')$, $h_2' = H_2(m', R', P_{ID}, R_{ID}', P_{pub})$, and $h_{ID}' = H_1(ID, P_{ID}, R_{ID}')$.

(iv) $\mathcal{A}_{II}$ assesses whether $gcd(l + h_1, n)$ equals 1. If it does not hold, the signer returns to step (i).

(v) As the the adversary is of Type II, the value of x is known. Then, $\mathcal{A}_{II}$ computes

$$s' = \left(t' + h_1'\right)^{-1} \left(r_{ID}' + h_{ID}' \cdot x + \frac{h_2' \cdot P_{ID}}{P}\right) \bmod n. \quad (8)$$

The signature is (R', s') on message m'.

(vi) To check the validity of the signature, the verifier can perform the following verification as follows:

$$s' \cdot \left(R' + h_1' \cdot P\right) = h_2' \cdot P_{ID} + R_{ID} + h_{ID}' \cdot P_{pub}, \quad (9)$$

where $h_1' = H_2(m', R', P_{ID}, R_{ID}')$, $h_2' = H_2(m', R', P_{ID}, R_{ID}', P_{pub})$, and $h_{ID}' = H_1(ID, P_{ID}, R_{ID}')$

$$\begin{aligned} & s' \cdot \left(R' + h_1' \cdot P\right) \\ &= \left(t' + h_1'\right)^{-1} \left(r_{ID}' + h_{ID}' \cdot x + \frac{h_2' \cdot P_{ID}}{P}\right) \\ &\quad \times \left(t' \cdot P + h_1' \cdot P\right) \\ &= \left(t' + h_1'\right)^{-1} \left(r_{ID}' + h_{ID}' \cdot x + \frac{h_2' \cdot P_{ID}}{P}\right) \left(t' + h_1'\right) \cdot P \\ &= \left(r_{ID}' + h_{ID}' \cdot x + \frac{h_2' \cdot P_{ID}}{P}\right) \cdot P \\ &= \left(r_{ID}' \cdot P + h_{ID}' \cdot x \cdot P + h_2' \cdot P_{ID}\right) \\ &= R_{ID}' + h_2' P_{ID} + h_{ID}' \cdot P_{pub}. \end{aligned} \quad (10)$$

5. Review of Fan et al.'s Short CLS Scheme

In this section, we briefly review the short certificateless signature scheme based on ECDLP [24]. The scheme works as follows.

Setup. Let G_1, G_2, and G_T be three cyclic additive groups of prime order $q \leq 2^k$ where k is a security parameter, and let e be an efficiently computable bilinear pairing $e : G_1 \times G_2 \to G_T$, which satisfies the properties of bilinearity and nondegeneracy. Suppose that a message m which will be signed is an element in Z_q^*. KGC chooses two random generators $P_1 \in G_1$ and $P_2 \in G_2$ and a random integer $s \in Z_q^*$. It then computes $P_{pub} = sP_2 \in G_2$ and $g = e(P_1, P_2) \in G_T$. It then selects two distinct cryptographic hash functions $H_1 : \{0,1\}^* \to Z_q^*$ and $H_2 : \{0,1\}^* \times G_2 \to Z_q^*$. KGC publishes the system parameters, params $= \{k, G_1, G_2, e, q, P, g, P_{pub}, H_1, H_2\}$, and keeps its master key s secret.

User-Key Gen. A user with identity ID randomly chooses $r \in Z_q^*$ and then computes $pk_{ID} = rP_2$ and $pk_{ID}' = r(P_{pub} + Q_{ID}P_2)$ where $Q_{ID} = H_1(ID)$. The user keeps r secretly and sets (pk_{ID}, pk_{ID}') as its public key.

Partial-Private-Key Gen. KGC takes params, the user's partial public information (Q_{ID}, pk_{ID}) as inputs, and then generates the user's partial-private key $d_{ID} = 1/(s + Q_{ID} + H_1(ID \parallel pk_{ID}))P_1$. Then KGC returns d_{ID} to the user via a secure manner. After receiving d_{ID}, the user checks the correctness of d_{ID} by examining if $e(d_{ID}, P_{pub} + Q_{ID}P_2 + H_1(ID \parallel pk_{ID})P_2) = g$. The private key of the user is (d_{ID}, r).

CL Sign. To produce the signature on message $m \in \{0,1\}^*$, the user with identity ID performs the following steps:

(i) set $h = H_2(m, pk_{ID})$,

(ii) compute $S = (1/(r + h))d_{ID}$, where S is the signature on message m of the user.

CL Verify. Given params, message m, pk_{ID}, pk_{ID}', and the signature S on message m of the user with identity ID, the signature can be verified as follows:

(i) let $h = H_2(m, pk_{ID})$;

(ii) if the following formula holds, the signature S is valid:

$$\begin{aligned} & e\left(S, pk_{ID}' + H_1\left(ID \parallel pk_{ID}\right) pk_{ID}\right. \\ &\quad \left. + h\left(P_{pub} + Q_{ID}P_2 + H_1\left(ID \parallel pk_{ID}\right) P_2\right)\right) = g. \end{aligned} \quad (11)$$

6. Cryptanalysis of Fan et al.'s Short CLS Scheme

In this section, we demonstrate that the Fan et al. [24] CLS scheme is forgeable by the Strong Type I adversary; that is, adversary can replace a user's public key but is not able to obtain KGCs master secret key. $\mathcal{A}_I$ is able to retrieve the partial-private key of the user.

6.1. Attack. The $\mathcal{A}_I$ will perform the following steps.

(i) The adversary $\mathcal{A}_I$ chooses a random number $r' \in Z_n^*$ and replaces a user's public key PK_{ID} with $PK_{ID}^* = r'P_2$ and PK_{ID}' with $PK_{ID}'^* = r'(P_{pub} + Q_{ID}P_2)$.

(ii) $\mathcal{A}_I$ makes a strong sign query with ID, m, and r' as input and then the challenger returns a valid signature $S' = (1/(r' + h'))d_{ID}$ where $h' = H_2(m, PK_{ID}^*)$.

(iii) $\mathcal{A}_I$ obtains the hash value h' on m, PK_{ID}^* by making a hash query.

(iv) $\mathcal{A}_I$ can then compute the user's partial-private key $d_{ID} = (r' + h')S'$ as he knows the value of r' and h'.

7. Conclusion

The schemes discussed here are of much interest because they are free from pairing and hence can easily be applicable to WSN. But less resource consumption is not enough reason to compromise security. In this paper, security attacks have been applied on two different schemes. Tsai et al. proposed the CLS scheme without pairing which is claimed to be more efficient than the existing schemes (since pairing is always an expensive operation). An exhaustive cryptanalysis has been shown in Section 4 and the results indicate that the improved scheme by Tsai et al. does not resist against the Strong Type II attacks and hence is forgeable. Moreover, we have found that Fan et al's. CLS scheme is forgeable by the Strong Type I adversary. Therefore, to construct a secure certificateless signature scheme without bilinear pairing needs more attention.

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] D. H. Yum and P. J. Lee, "Generic constructin of certificateless signature," in *Information Security and Privacy*, vol. 3108 of *Lecture Notes in Computer Science*, pp. 200–211, Springer, Berlin, Germany, 2004.

[5] B. C. Hu, D. S. Wong, Z. Zhang, and X. Deng, "Key replacement attack against a generic construction of certificateless signature," in *Information Security and Privacy*, vol. 4058 of *Lecture Notes in Computer Science*, pp. 235–246, Springer, Berlin, Germany, 2006.

[6] 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.

[7] 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.

[8] 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/.

[9] 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.

[10] Z. Zhang, D. S. Wong, J. Xu, and D. Feng, "Certificateless public-key signature: security model and efficient construction," in *Applied Cryptography and Network Security*, vol. 3989 of *Lecture Notes in Computer Science*, pp. 293–308, Springer, Berlin, Germany, 2006.

[11] W. S. Yap, S. H. Heng, and B. M. Goi, "An efficient certificateless signature scheme," in *Emerging Directions in Embedded and Ubiquitous Computing*, vol. 4097 of *Lecture Notes in Computer Science*, pp. 322–331, Springer, Berlin, Germany, 2006.

[12] J. Park and B. Kang, "Security analysis of the certificateless signature scheme proposed at Sec Ubiq 2006," in *Emerging Directions in Embedded and Ubiquitous Computing*, vol. 4809 of *Lecture Notes in Computer Science*, pp. 686–691, Springer, Berlin, Germany, 2007.

[13] M. H. Au, J. Chen, J. K. Liu, Y. Mu, D. S. Wong, and G. Yang, "Malicious KGC attacks in certificateless cryptography," in *Proceedings of the 12th Australasian Conference on Information Security and Privacy (ACISP '07)*, vol. 4586 of *Lecture Notes in Computer Science*, pp. 308–322, Springer, 2007.

[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. 308–322, Springer, Berlin, Germany, 2007.

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

[16] R. Tso, X. Yi, and X. Huang, "Efficient and short certificateless signature," in *Cryptology and Network Security*, vol. 5339 of *Lecture Notes in Computer Science*, pp. 64–79, Springer, Berlin, Germany, 2008.

[17] R. Tso, X. Yi, and X. Huang, "Efficient and short certificateless signatures secure against realistic adversaries," *Journal of Supercomputing*, vol. 55, no. 2, pp. 173–191, 2011.

[18] R. Tso, X. Huang, and W. Susilo, "Strongly secure certificateless short signatures," *Journal of Systems and Software*, vol. 85, no. 6, pp. 1409–1417, 2012.

[19] 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, chn, June 2008.

[20] 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.

[21] 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.

[22] C. Wang, D. Long, and Y. Tang, "An efficient certificateless signature from pairings," *Journal of Information Science and Engineering*, vol. 8, no. 1, pp. 96–100, 2009.

[23] H. Du and Q. Wen, "Efficient and provably-secure certificateless short signature scheme from bilinear pairings," *Computer Standards and Interfaces*, vol. 31, no. 2, pp. 390–394, 2009.

[24] C. Fan, R. Hsu, and P. Ho, "Truly non-repudiation certificateless short signature scheme from bilinear pairings," *Journal of Information Science and Engineering*, vol. 27, no. 3, pp. 969–982, 2011.

[25] 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.

[26] Y. C. Chen and G. Horng, "On the security models for certificateless signature schemes achieving level 3 security," IACR Cryptology EPrint Archive 554, 2011.

[27] M. Tian, L. Huang, and W. Yang, "On the security of a certificateless short signature scheme," Cryptology EPrint Archive, 2011, http://eprint.iacr.org/2011/419.

[28] X. Huang, Y. Mu, W. Susilo, D. S. Wong, and W. Wu, "Certificateless signatures: new schemes and security models," *Computer Journal*, vol. 55, no. 4, pp. 457–474, 2012.

[29] D. He, J. Chen, and R. Zhang, "An efficient and provably-secure certificateless signature scheme without bilinear pairings," *International Journal of Communication Systems*, vol. 25, no. 11, pp. 1432–1442, 2011.

[30] M. Tian and L. Huang, "Cryptanalysis of a certificateless signature scheme without pairings," *International Journal of Communication Systems*, 2012.

[31] J. Tsai, N. Lo, and T. Wu, "Weaknesses and improvements of an efficient certificateless signature scheme without using bilinear pairings," *International Journal of Communications Systems*, vol. 25, no. 11, pp. 1432–1442, 2012, Wiley-Blackwell.

[32] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.

[33] "2000. *Standards for efficient cryptography SEC 1: Elliptic curve cryptography*," Certicom Research, http://www.secg.org/collateral/sec1_final.pdf.

[34] "2000. *Standards for efficient cryptography SEC 2: Recommended Elliptic Curve Domain Parameters. Standards for Efficient Cryptography*," Version 1.0. Certicom Research, http://www.secg.org/collateral/sec2_final.pdf.

[35] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer, New York, NY, USA, 2004.