Hindawi
Security and Communication Networks
Volume 2022, Article ID 6174031, 6 pages
https://doi.org/10.1155/2022/6174031

Research Article

Cryptanalysis of a Certificateless Hybrid Signcryption Scheme and a Certificateless Encryption Scheme for Internet of Things

Shan Shan

School of Economics and Management, Shandong Jiaotong University, Jinan 250357, China

Correspondence should be addressed to Shan Shan; jtshanshan@126.com

Received 9 April 2022; Revised 13 June 2022; Accepted 29 June 2022; Published 13 July 2022

Academic Editor: Jie Cui

In wireless and mobile networks with limited storage and computing resources, certificateless cryptography has more advantages because of its low dependence on infrastructure and short security parameters. Recently, Gong et al. and Karati et al., respectively, proposed a new certificateless scheme in the Internet of Things environment, one of which is a certificateless hybrid signcryption scheme, and the other's basis is a certificateless encryption scheme. Gong et al. and Karati et al. gave the formal security proof for their schemes, respectively. In this article, the attack algorithms against these two schemes are presented separately, thus proving that their schemes are insecure and not suitable for the Internet of Things environment.

1. Introduction

The primary problem to be solved in public key cryptography is how to certify the ownership of key pairs. In certificate-based public key infrastructure (PKI), a trusted third party called certificate authority (CA) issues certificates that provide a trusted link between the user's identity and the public key based on digital signature technology. However, certificate management is very complex. Shamir [1] proposed the concept of an identity-based cryptosystem in 1984 to simplify certificate management issues. The main idea is that you can easily export a user's public key from any string that corresponds to the user's identifying information, such as name, phone number, and E-mail address. A private key generator (PKG) calculates the private keys using the master key and securely distributes these private keys to the users participating in the scheme. From an efficiency and convenience standpoint, an identity-based system may be a good alternative to a certificate-based system. But key escrow, which means the user's private key is generated and known by PKG, is an inherent problem resulting in no authenticity and no privacy for the user in an identity-based system.

As a variant of the identity-based cryptosystem, the concept of certificateless was proposed in 2003 to eliminate these problems simultaneously [2]. Each user in a certificateless scheme independently generates a secret key and gets another partial private key from the key generation center (KGC). Thus, each user's secret consists of two parts, one obtained from a trusted third party (KGC) and one generated by the user himself. Certificateless scheme successfully solves the key escrow problem. In addition, this kind of scheme does not require the trusted third party to authenticate the corresponding public key ownership, which makes public key management very efficient. Because of these advantages, certificateless schemes have attracted wide attention and become one of the hot topics of public key cryptography. In recent years, certificateless signcryption [3, 4], certificateless hybrid signcryption [5, 6], certificateless multireceiver signcryption [7–9], certificateless generalized signcryption [10–14], and certificateless online/offline signcryption [15, 16] have been put forward one after another.

In wireless and mobile networks with limited storage and computing resources, certificateless cryptography has more advantages because of its low dependence on infrastructure and short security parameters. However, while achieving low computational costs, many certificateless schemes proposed in the Internet of things environment [17–23] cannot simultaneously provide provable security. Kumar et al. [17]

claimed that their newly proposed certificateless aggregate signature scheme is secure against both types of attackers. Zhan and Wang [24] proved that an attacker could forge a valid signature and valid aggregate signature. Lin et al. [25] pointed out that the certificateless signcryption (CL-SC) scheme proposed by Rastegari et al. [18] is insecure. Zhan et al. [26] analyzed a pairing-free CLAS scheme proposed in [20] and pointed out that the scheme is insecure. On this basis, to solve the security vulnerability, an improved scheme was proposed at the same time. Khan et al. [21] proposed a certificateless offline/online signature scheme. Unfortunately, their scheme is not secure against adaptive selective message attacks. Hussain et al. [27] proved that an adversary could forge a valid signature on a message by replacing a public key. Kasyoka et al. [28] showed the security vulnerabilities of Wei and Ma's [19] signcryption scheme and proposed corresponding modifications to show how their scheme could be made more secure. Xu and Zeng [29] pointed out that the certificateless aggregate arbitrated signature scheme proposed by Lee et al. [22] is not secure for type-1 attackers that can replace user public keys. They also showed that Addobea et al.'s [23] offline-online certificateless signature scheme cannot achieve correctness. Therefore, the certificateless solution described above cannot be deployed in real Internet of things environment and mobile applications. Most of the schemes fail because the definition of the security model is not complete, and in the proving process, the adversary capability is not successfully reduced to solve difficult problems. There has been an ongoing effort in the Internet of things to make greater advances in security and performance.

1.1. Our Contributions. Recently, Gong et al. [30] and Karati et al. [31], respectively, proposed a new certificateless scheme in the Internet of things environment, one of which is a certificateless hybrid signcryption scheme, and the other's basis is a certificateless encryption scheme. Their schemes were claimed to be secure, and the formal security was presented which reducing adversary capabilities in solving difficult problems. It is a pity that Gong et al.'s scheme and Karati et al.'s scheme are not secure in the case of internal attacks as shown in this paper. The attack algorithms against these two schemes are presented separately, thus proving that their schemes are insecure and not suitable for the Internet of things environment.

1.2. Paper Organization. In Section 2, we give the cryptanalysis of Gong et al.'s scheme, and we give the cryptanalysis of Karati et al.'s certificateless encryption scheme for the industrial Internet of things in Section 3. Section 4 provides a conclusion.

2. Cryptanalysis of Gong et al.'s Certificateless Hybrid Signcryption Scheme

Because of the limitation of symmetric cryptography, public key-based authentication technology has attracted extensive attention. It provides secure communication and accesses mechanism for various applications. Compared with single-factor or two-factor protocols, multifactor schemes have been proven to achieve higher security levels. Wang et al. [32–34] have made a series of representative achievements in multifactor authentication. However, in some applications, people have to strike a balance between availability and security and adopt single-factor technology to achieve authentication, such as digital signature and digital signcryption. Signcryption can provide confidentiality and authentication at the same time and is widely used in many applications where multiple security features are required. Gong et al.'s scheme is a concrete certificateless hybrid signcryption scheme.

2.1. Gong et al.'s Scheme. As shown below, their scheme includes five algorithms altogether: Setup, Extract-Partial-Private-Key, Generate-User-Keys, Signcrypt, and Unsigncrypt.

2.1.1. Setup. KGC runs the following algorithms:

(i) Generate two distinct cyclic groups G_1 (an additive cyclic group with a generator P) and G_2 (a multiplicative cyclic group) of prime order $q\,(q \geq 2^{\gamma})$. e is a bilinear map.

(ii) Chooses $x \in_R Z_q^*$, computes $P_{\text{pub}} = e(P, P)^x$.

(iii) Chooses one-way hash functions as h_1: $\{0,1\}^* \longrightarrow Z_q^*$, h_2: $\{0,1\}^{*2} \times G_1 \times G_2^2 \longrightarrow Z_q^*$, h_3: $Z_q^* \longrightarrow Z_q^*$, h_4: $G_2 \times Z_q^* \times G_1 \longrightarrow \{0,1\}^n$, h_5: $G_1 \longrightarrow Z_q^*$.

(iv) Finally, keeps x safely and outputs params = $\{P, P_{\text{pub}}, G_1, G_2, q, e, n, h_i, E, D\}$ as the system parameter.

2.1.2. Extract-Partial-Private-Key. Given the identity information u_i, to generate the corresponding partial private key d_i, KGC runs the following algorithms:

(i) Computes $Q_i = h_1(u_i)$

(ii) Sets the partial private key $d_i \leftarrow x h_1(u_i)$

2.1.3. Generate-User-Keys. The user chooses $x_i \in_R Z_q^*$ and computes $P_i = e(P, P)^{x_i}$ which is the public key and sets the full private key $s_i = (x_i, d_i)$.

2.1.4. Signcrypt. A sender u_A runs the following algorithms to generate the ciphertext.

(i) Chooses $r \in_R Z_q^*$

(ii) Computes $R = rP$, $y = P_B^{x_A h_5(R)}$ and $z = h_3(Q_B \cdot d_A)$, where $Q_B = h_1(u_B)$

(iii) Computes $K = h_4(y, z, R)$ and $c = Enc_K(m)$

(iv) Computes $f = h_2(u_A, u_B, R, P_A, P_B)$ and $s = r \cdot z / x_A \cdot f$

(v) Outputs $\sigma = (c, R, s)$ as the ciphertext

2.1.5. Unsigncrypt. A receiver u_B runs the following algorithms for unsigncryption.

(i) Computes $y = P_A^{x_B h_5(R)}$, $z = h_3(Q_A \cdot d_B)$, $Q_A = h_1(u_A)$ and $K = h_4(y, z, R)$.
(ii) Computes message $m/\perp \leftarrow Dec_K(c)$. If output $\perp$, u_B refuses the message.
(iii) Computes $f = h_2(u_A, u_B, R, P_A, P_B)$.
(iv) Checks $P_A^{s \cdot f} = e(zP, R)$ holds or not. If it holds, u_B get m, else u_B refuses the message.

2.2. Cryptanalysis of Gong et al.'s Scheme

2.2.1. Attack Algorithm 1 (Internal Attacks to the Unforgeability). Once receives a valid signcryption text $\sigma = (c, R, s)$, the receiver can impersonate the sender to generate signcryption text for any message m' sent to him. The attack algorithm is described as follows:

(i) Chooses $r' \in_R Z_q^*$
(ii) Computes $R' = r'R$, $z = h_3(Q_A \cdot d_B)$, and $f = h_2(u_A, u_B, R, P_A, P_B)$
(iii) Computes $y' = P_A^{x_B h_5(R')}$, $z' = h_3(Q_A \cdot d_B)$, where $Q_A = h_1(u_A)$
(iv) Computes $K' = h_4(y', z', R')$
(v) Computes $c' = Enc_{K'}(m')$
(vi) Computes $f' = h_2(u_A, u_B, R', P_A, P_B)$ and $s' = s \cdot f/z \cdot r' \cdot z'/f'$
(vii) Send the ciphertext $\sigma' = (c', R', s')$ of message m'

2.2.2. Correctness. The signcryption ciphertext $\sigma' = (c', R', s')$ is validly related with m' as shown in the following.

Since $R' = r'R = r' \cdot r \cdot P$, $y' = P_A^{x_B h_5(R')} = P_B^{x_A h_5(R')}$, $z' = h_3(Q_A \cdot d_B) = h_3(Q_B \cdot d_A)$, the receiver can compute $m' = \mathrm{Dec}_{K'}(c')$ where $K' = h_4(y', z', R')$.

The equation $P_A^{s' \cdot f'} = e(z'P, R')$ always holds since

$$\begin{aligned} s' &= s \cdot \frac{f}{z} \cdot r' \cdot \frac{z'}{f'}, \\ &= \frac{r \cdot z}{x_A \cdot f} \cdot \frac{f}{z} \cdot r' \cdot \frac{z'}{f'}, \\ &= \frac{r \cdot r' \cdot z'}{x_A \cdot f'}, \end{aligned} \quad (1)$$

$$\begin{aligned} P_A^{s' \cdot f'} &= e(P, P)^{x_A \cdot \frac{r \cdot r' \cdot z'}{x_A \cdot f'} \cdot f'} \\ &= e(P, P)^{r \cdot r' \cdot z'} \\ &= e(z'P, r \cdot r' \cdot P) \\ &= e(z'P, R'). \end{aligned} \quad (2)$$

Thus, $\sigma' = (c', R', s')$ is a valid signcryption ciphertext.

Any user can launch the attack after receiving a valid signcryption ciphertext sent to him, so the nonrepudiation and source authentication that should be satisfied by the digital signcryption scheme cannot be realized.

2.2.3. Attack Algorithm 2 (Internal Attacks to the Master Secret Key). As shown in the Extract-Partial-Private-Key algorithm, KGC generates d_i by computing $Q_i = h_1(u_i)$ and $d_i \leftarrow x h_1(u_i)$.

Since x is a random element in Z_q^* and h_1 is a hash function that maps strings to distinct elements in Z_q^*, any partial private key holder can compute the master secret key x by $x = d_i \cdot h_1^{-1}(u_i) \in Z_q^*$ directly. Any security of the whole system cannot be realized when the master secret key is leaked. Any user that receives a valid partial private key can launch the attack.

3. Cryptanalysis of Karati et al.'s Certificateless Encryption Scheme

In order to achieve more complex security goals, people often adopt the method of extending features on the basis of the general scheme. Karati et al.'s reliable data sharing protocol is based on a certificateless encryption scheme.

3.1. Karati et al.'s Scheme. As shown below, their scheme includes ten algorithms: Setup, Set-Secret-Value, Set-Public-Value, Set-Partial-Private-Key, Set-Full-Public-Key, Set-Full-Private-Key, Encrypt, Gen-TrapdoorTest-Trapdoor, and Decrypt.

3.1.1. Setup. KGC runs the following algorithms.

(i) Generates three distinct cyclic groups G_1, G_2, and G_3, and $e: G_1 \times G_2 \longrightarrow G_3$ is a bilinear map
(ii) Chooses generator $g \in G_1, h \in G_2$
(iii) Chooses $H_1: \{0,1\}^* \times G_1 \times G_2 \times G_3 \longrightarrow \mathbb{Z}_p^*$, $H_2: \{0,1\}^* \longrightarrow \mathbb{Z}_p^*$, and $H_3: G_3 \longrightarrow \{0,1\}^{n_1+n_2}$ for some n_1 and n_2, which are one-way hash functions
(iv) Computes $g_1 = g^{x_{KGC}}$ for $x_{KGC} \in_R \mathbb{Z}_p^*$
(v) Keeps $MSK = (x_{KGC})$ safely and publishes params $= \{p, g, g_1, h, H_i\}$

3.1.2. Set-Secret-Value and Set-Public-Value

(i) Chooses $y_i \in_R \mathbb{Z}_p^*$ and sets secret-value $SS_i = (y_i)$
(ii) Generates public value $PV_i = (P_{i1} = h^{y_i}, \; P_{i2} = e(g, h)^{1/y_i})$

3.1.3. Set-Partial-Private-Key. KGC runs the following algorithms to generate the partial private key of device i:

(i) Chooses $\beta_i \in_R \mathbb{Z}_p^*$ and $d_i \in_R \mathbb{Z}_p^*$
(ii) Computes $P_{i3} = g^{\beta_i}$ and $\alpha_i = H_1(ID_i, P_{i3}, P_{i1}, P_{i2})$
(iii) Computes $x_i = 1/(\alpha_i \beta_i + d_i x_{KGC})$ and $D_i' = h^{x_i}$

(iv) Outputs $PP_i = (d_i, P_{i3}, D_i')$

On receiving PP_i securely, device i may check it by the equation $e(P_{i3}^{\alpha_i} \cdot g_1^{d_i}, D_i') = e(g, h)$.

3.1.4. Set-Full-Public-Key and Set-Full-Private-Key. The full public key of Device i can be expressed as $PK_i = (P_{i1}, P_{i2}, P_{i3})$, and the full private key can be expressed as $SK_i = (y_i, d_i, D_i = D_i'^{1/y_i})$.

3.1.5. Encrypt. Given the message m_i and keyword $w_{ij} \in \{0,1\}^{n_3}$, a sender, whose private key is SK_s, runs the following algorithms to generate a ciphertext sending to receiver R with public key PK_r.

(i) Chooses $u \in_R \mathbb{Z}_p^*$ and $\sigma \in_R \{0,1\}^{n_2}$

(ii) Sets $C_i = (c_{i1} = P_{r3}^{u\alpha_r}, c_{i2} = g_1^u, c_{i3} = (m_i \| \sigma) \oplus H_3(P_{r2}^u))$

(iii) Computes $v = H_1((\sigma \| w_{ij} \| y_s), g, h, P_{s2})$, $\Phi_{ij} = (\phi_{ij1}, \phi_{ij2})$, where $\phi_{ij1} = [g_1 \cdot g^{H_2(w_{ij} \| \alpha_s \| \alpha_r)}]^v$ and $\phi_{ij2} = P_{r1}^{v y_s}$

(iv) Outputs $(C_i, \Phi_{ij}, \theta_{ij})$ for $\theta_{ij} = H_2(m_i \| \sigma \| w_{ij})$

3.1.6. Gen-Trapdoor. Given a tester's private-public key pair $(t \in_R \mathbb{Z}_p^*, \langle P_{t1} = h', P_{t2} = e(g,h)^{1/t} \rangle)$, receiver R runs the following algorithms to generate a trapdoor $\Gamma_{ik} = (\tau_{ik1}, \tau_{ik2})$.

(i) Computes $v' = H_1((\sigma' \| w_{ik} \| y_r), g, h, P_{r2})$

(ii) Computes $\tau_{ik1} = [g_1 \cdot g^{H_2(w_{ik} \| \alpha_s \| \alpha_r)}]^{v'}$ and $\tau_{ik2} = P_{s1}^{v' y_r / H_1(\alpha_r, g, P_{t1}^{y_r}, P_{r2})}$ for $\sigma' \in \{0,1\}^{n_1}$

3.1.7. Test-Trapdoor. The tester computes $v'' = H_1(\alpha_r, g, P_{r1}^t, P_{r2})$ and retrieves C_i if the condition $e(\phi_{ij1}, \tau_{ik2})^{v''} = e(\tau_{ik1}, \phi_{ij2})$ holds.

3.1.8. Decrypt. Given a keyword w_{ik}, $SK_r = (y_r, d_r, D_r)$, C_i, the receiver computes $\delta_2 = e(c_{i1} c_{i2}^{d_r}, D_r)$ and $\delta_1 = (m_i \| \sigma) = c_{i3} \oplus H_3(\delta_2)$. The first n_1 bit of δ_1 is returned as m_i' if $\theta_{ij} = H_2(\delta_1 \| w_{ik})$.

3.2. Cryptanalysis of Karati et al.'s Scheme. To show the usability, Karati et al. defined their scheme as (M, C, W, Γ)-KDCLEKS. We noticed that if the sender sends a message directly without any keyword, $(M, C, \perp, \perp)$-KDCLEKS is a common certificateless encryption scheme, which can be marked as (M, C)-KDCLEKS.

In this section, it will be shown that the encryption algorithm (M, C)-KDCLEKS is not secure under public-key replacement attacks launched by an adversary $\mathbb{A}_I$.

3.2.1. Attack Algorithm 1 (Internal Attacks to the Partial Private Key). Assume the following conditions a user declares his public value as $PV_j = (P_{j1} = h^{y_j}, P_{j2} = e(g,h)^{1/y_j})$. Once $\mathbb{A}_I$ receives a valid partial private key $PP_i = (d_i, P_{i3}, D_i')$, it can calculate and generate a partial private key for this user as follows:

(1) Compute $P_{j3} = P_{i3}^{\alpha_i}$ and $\alpha_j = H_1(ID_j, P_{j3}, P_{j1}, P_{j2})$

(2) Compute $d_j = \alpha_j \cdot d_i$

(3) Compute $D_j' = D_i'^{1/\alpha_j}$

3.2.2. Correctness. $PP_j = (d_j, P_{j3}, D_j')$ is a valid partial private key related to public value PV_j as shown in the following equation:

$$
\begin{aligned}
& e\left(P_{j3}^{\alpha_j} \cdot g_1^{d_j}, D_j'\right) \\
& = e\left(P_{i3}^{\alpha_i \alpha_j} \cdot g_1^{\alpha_j \cdot d_i}, D_i'^{1/\alpha_j}\right) \\
& = e\left(g^{\beta_i \alpha_i} \cdot g_1^{d_i}, h^{x_i}\right) \\
& = e\left(g^{\alpha_i \beta_i} \cdot g^{d_i x_{KGC}}, h^{1/(\alpha_i \beta_i + d_i x_{KGC})}\right) \\
& = e(g, h).
\end{aligned} \tag{3}
$$

Thus, $PP_j = (d_j, P_{j3}, D_j')$ can always be accepted as a valid partial private key related to public value PV_j. Any user that receives a valid partial private key can launch the attack. This means that the user's partial private key can be forged, leading to the lack of availability.

3.2.3. Attack Algorithm 2 (Internal Attacks to the Confidentiality). Once $\mathbb{A}_I$ receives a valid Full-Public-Key $PK_i = (P_{i1}, P_{i2}, P_{i3})$ and corresponding Full-Private-Key $SK_i = (y_i, d_i, D_i)$, he can decrypt the ciphertext of any user J with ID_j through public key replacement attacks. The attack algorithm is described as follows:

(1) Select random parameter $y' \in_R \mathbb{Z}_p^*$, and compute $P_{j1} = P_{i1}^{y'} = h^{y_i \cdot y'}$, $P_{j2} = P_{i2}^{1/y'} = e(g,h)^{1/(y_i \cdot y')}$ and $P_{j3} = P_{i3}^{\alpha_i}$ where $\alpha_i = H_1(ID_i, P_{i3}, P_{i1}, P_{i2})$

(2) Replace the public key of user J with the value $PK_j = (P_{j1}, P_{j2}, P_{j3})$

On inputs *params* and receiver J' s public key PK_J with message $m_j \in \{0,1\}^{n_1}$, the sender selects $\sigma \in_R \{0,1\}^{n_2}$, $u \in_R \mathbb{Z}_p^*$ and sets $C_j = (c_{j1}, c_{j2}, c_{j3})$, where $c_{j1} = P_{j3}^{u\alpha_j}$, $c_{j2} = g_1^u$, $c_{j3} = (m_j \| \sigma) \oplus H_3(P_{j2}^u)$ where $\alpha_j = H_1(ID_j, P_{j3}, P_{j1}, P_{j2})$. Finally, the sender outputs C_j as the ciphertext.

Given the ciphertext C_j, $\mathbb{A}_I$ can successfully decrypt it using the following algorithm:

(1) Compute $\alpha_j = H_1(ID_j, P_{j3}, P_{j1}, P_{j2})$

(2) Compute $y_j = y_i \cdot y'$, $d_j = \alpha_j \cdot d_i$, $D_j = D_i'^{1/(\alpha_j \cdot y_i \cdot y')}$

(3) Compute $\delta_1 = (m_j \| \sigma) = c_{j3} \oplus H_3(\delta_2)$, where $\delta_2 = e(c_{j1} c_{j2}^{d_j}, D_j)$

3.2.4. Correctness. The decryption process is always successful as shown in the following equation:

$$\begin{aligned}
\delta_2 &= e\left(c_{j1}c_{j2}^{d_j}, D_j\right) \\
&= e\left(P_{i3}^{u\cdot\alpha_i\alpha_j}\cdot g_1^{u\cdot d_j}, D_i^{\prime 1/\left(\alpha_j\cdot y_i\cdot y'\right)}\right) \\
&= e\left(g^{u\cdot\left(\beta_i\alpha_i\alpha_j+x_{KGC}d_j\right)}, h^{x_i/\left(\alpha_j\cdot y_i\cdot y'\right)}\right) \\
&= e\left(g^{u\cdot\left(\beta_i\alpha_i\alpha_j+x_{KGC}\alpha_j d_i\right)}, h^{1/\left(\left(\beta_i\alpha_i\alpha_j+x_{KGC}\alpha_j d_i\right)y_i\cdot y'\right)}\right) \\
&= e(g,h)^{u/\left(y_i\cdot y'\right)} = P_{j2}^u.
\end{aligned} \tag{4}$$

Thus, $\mathbb{A}_I$ reveals $m_j\|\sigma = c_{j3}\oplus H_3(\delta_2)$ with probability 1. This attack can be launched by a user who receives any legal partial private key sent to him, and he can decrypt the ciphertext of any user through public key replacement attacks without knowing the master secret MSK. This means that any user's public key can be replaced, and the message can be revealed by the attacker, leading to the lack of confidentiality.

4. Conclusion

Gong et al. gave a formal security proof in the random oracle model, and Karati et al. proved their scheme is secure against adversaries. Unfortunately, we noticed that in Gong et al.'s scheme, internal users can forge the signcryption ciphertext sent to them, the nonrepudiation and source authentication that should be satisfied by the digital signcryption scheme cannot be realized. The more serious is that any partial private key holder can directly calculate the master secret key, which leads to the failure to implement security features. Any user who obtains a partial private key in Karati et al.'s basic certificateless encryption scheme can either forge the partial private key of another user or replace the public key of another user to decrypt the ciphertext. Therefore, their solutions are insecure and not suitable for the Internet of things environment.

Data Availability

All data generated or analyzed during this study are included in this published article.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] A. Shamir, "Identity-based cryptosystem and signature scheme," in *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques*, pp. 120–126, Paris, France, April 1984.

[2] S. Al-Riyami and K. Paterson, "Certificateless public key cryptography," in *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*, pp. 452–474, Taipei, Taiwan, December 2003.

[3] M. Barbosa and P. Farshim, "Certificateless signcryption," in *Proceedings of the ACM Symposium on Information, Computer and Communications Security-ASIACCS*, pp. 369–372, New York, NY, USA, March 2008.

[4] H. Yang and B. Yang, "Pairing-free and secure certificateless signcryption scheme," *The Computer Journal*, vol. 60, no. 8, pp. 1187–1196, 2017.

[5] F. Li, M. Shirase, and T. Takagi, "Certificateless hybrid signcryption," in *Proceedings of the 5th International Conference on Information Security Practice and Experience*, pp. 112–123, Nanjing, China, December 2009.

[6] A. Liang and H. Liang, "Certificateless hybrid signcryption scheme for secure communication of wireless sensor networks," *Wireless Personal Communications*, vol. 80, no. 3, pp. 1049–1062, 2015.

[7] S. Selvi, D. Shukla, and P. R. Chandrasekaran, "Efficient and provably secure certificateless multi-receiver signcryption,"vol. 5324, pp. 52–67, in *Proceedings of the Provable Security Second International Conference, ProvSec*, vol. 5324, pp. 52–67, Springer, Berlin, Germany, October 2008.

[8] J. Qiu, K. Fan, K. Zhang, Q. Pan, H. Li, and Y. Yang, "An efficient multi-message and multi-receiver signcryption scheme for heterogeneous smart mobile IoT," *IEEE Access*, vol. 7, pp. 180205–180217, 2019.

[9] C. Peng, J. Chen, M. S. Obaidat, P. Vijayakumar, and D. He, "Efficient and provably secure multireceiver signcryption scheme for multicast communication in edge computing," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6056–6068, 2020.

[10] C. Zhou, Z. Zhao, and W. Zhou, "Certificateless key insulated generalized signcryption scheme without bilinear pairings," *Security and Communication Networks*, vol. 2017, Article ID 8405879, 9 pages, 2017.

[11] A. Zhang, L. Wang, X. Ye, and X. Lin, "Light-weight and robust security-aware d2d-assist data transmission protocol for mobile-health systems," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 3, pp. 662–675, 2017.

[12] B. Zhang, Z. Jia, and C. Zhao, "An efficient certificateless generalized signcryption scheme," *Security and Communication Networks*, vol. 2018, Article ID 3578942, 13 pages, 2018.

[13] A. Karati, C. I. Fan, and R. H. Hsu, "Provably secure and generalized signcryption with public verifiability for secure data transmission between resource-constrained IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10431–10440, 2019.

[14] C. Zhou, "An improved lightweight certificateless generalized signcryption scheme for mobile-health system," *International Journal of Distributed Sensor Networks*, vol. 15, no. 1, Article ID 155014771882446, 2019.

[15] J. Li, J. Zhao, and Y. Zhang, "Certificateless online/offline signcryption scheme," *Security and Communication Networks*, vol. 8, no. 11, pp. 1979–1990, 2015.

[16] F. Li, Y. Han, and C. Jin, "Certificateless online/offline signcryption for the Internet of Things," *Wireless Networks*, vol. 23, no. 1, pp. 145–158, 2017.

[17] P. Kumar, S. Kumari, V. Sangaiah, A. K. Wei, J. Li, and X. Li, "A certificateless aggregate signature scheme for healthcare wireless sensor network," *Sustainable Computing: Informatics and Systems*, vol. 18, pp. 80–89, 2018.

[18] P. Rastegari, W. Susilo, and M. Dakhlalian, "Efficient certificateless signcryption in the standard model: revisiting Luo and Wan's scheme from wireless personal communications," *Computer Journal*, vol. 62, no. 8, pp. 1178–1193, 2018.

[19] L. Wei and W. Ma, "Secure and efficient data sharing scheme based on certificateless hybrid signcryption for cloud storage," *MDPI-Electronics.*vol. 8, no. 590, pp. 1–12, 2019.

[20] J. Liu, L. Yu, and Y. Yu, "Improved security of a pairing-free certificateless aggregate signature in healthcare wireless medical sensor networks," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5256–5266, 2020.

[21] M. A. Khan, S. U. Rehman, M. I. Uddin et al., "An online-offline certificateless signature scheme for internet of health things," *Journal of Healthcare Engineering*, vol. 2020, Article ID 6654063, 10 pages, 2020.

[22] D. H. Lee, K. Yim, and I. Y. Lee, "A certificateless aggregate arbitrated signature scheme for iot environments," *Sensors*, vol. 20, no. 14, p. 3983, 2020.

[23] A. A. Addobea, J. Li, and Q. Li, "MHCOOS: an offline-online certificateless signature scheme for M-health devices," *Security and Communication Networks*, vol. 2020, Article ID 7085623, 12 pages, 2020.

[24] Y. Zhan and B. Wang, "Cryptanalysis of a certificateless aggregate signature scheme for healthcare wireless sensor network," *Security and Communication Networks*, vol. 2019, Article ID 6059834, 5 pages, 2019.

[25] X. J. Lin, L. Sun, Z. Zhang, X. Qu, and H. Qu, "On the security of a certificateless signcryption with known session-specific temporary information security in the standard model," *The Computer Journal*, vol. 63, no. 8, pp. 1259–1262, 2020.

[26] Y. Zhan, B. Lu, and R. Lu, "Cryptanalysis and improvement of a pairing-free certificateless aggregate signature in healthcare wireless medical sensor networks," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5973–5984, 2021.

[27] S. Hussain, S. Sajid Ullah, M. Shorfuzzaman, M. Uddin, and M. Kaosar, "Cryptanalysis of an online/offline certificateless signature scheme for internet of health things," *Intelligent Automation & Soft Computing*, vol. 30, no. 3, pp. 983–993, 2021.

[28] P. Kasyoka, M. Angolo, and S. M. Angolo, "Cryptanalysis of a pairing-free certificateless signcryption scheme," *Ict Express*, vol. 7, no. 2, pp. 200–204, 2021.

[29] F. Xu and H. Zeng, "Cryptanalysis of two signature schemes for IOT and mobile health systems," *Wireless Personal Communications*, vol. 122, no. 3, pp. 2035–2043, 2022.

[30] B. Gong, Y. Wu, Q. Ren, Yh Guo, and C. Guo, "A secure and lightweight certificateless hybrid signcryption scheme for Internet of Things," *Future Generation Computer Systems*, vol. 127, pp. 23–30, 2022.

[31] A. Karati, C. I. Fan, and E. S. Zhuang, "Reliable data sharing by certificateless encryption supporting keyword search against vulnerable KGC in Industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 6, pp. 3661–3669, 2022.

[32] D. Wang, H. Cheng, D. Wang, and P. Wang, "On the challenges in designing identity-based privacy-preserving authentication schemes for mobile devices," *IEEE Systems Journal*, vol. 12, no. 1, pp. 916–925, 2018.

[33] S. Qiu, D. Wang, G. Kumari, and S. Kumari, "Practical and provably secure three-factor Authentication protocol based on extended chaotic-maps for mobile lightweight devices," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, pp. 1338–1351, 2020.

[34] Q. Wang, D. Wang, C. He, and D. He, "Quantum2FA: efficient quantum-resistant two-factor Authentication scheme for mobile devices," *IEEE Transactions on Dependable and Secure Computing*, p. 1, 2022.