Cross domain heterogeneous signcryption scheme with equality test for WBAN

Ming Luo (lmhappy21@163.com)
Nanchang University https://orcid.org/0000-0002-2231-3775
Yusi Pei
Nanchang University
Minrong Qiu
Nanchang University

Research Article

Keywords: Wireless body area network, Cross domain heterogeneous, Signcryption, Equality test

Posted Date: August 8th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1928854/v1

Cross domain heterogeneous signcryption scheme with equality test for WBAN

Ming Luo[1] · Yusi Pei[1] · Minrong Qiu[2]

Abstract

The rapid development of wireless sensors has accelerated the popularity of wireless body area network (WBAN). WBAN use multiple sensors to collect the patient's body data, and the data is transferred to the medical cloud for processing and analyzing. In order to protect the data in the medical cloud, some heterogeneous signcryption schemes that support equality test have been proposed. However, we observe that these schemes use the same cryptographic parameters in different cryptographic systems. In addition, most of these schemes cannot resist the replay attack (RRA) or know session temporary key attack (RKSTKA). To deal with these problems, this paper presents a cross domain heterogeneous signcryption scheme with equality test (CDSCET) for WBAN. In CDSCET, the ciphertexts are from certificateless cryptographic system (CLC) to public key infrastructure (PKI), where two different cryptosystems use different cryptographic parameters. CDSCET can realize confidentiality, integrity, authentication, RRA and RKSTKA. Moreover, compared with three latest schemes, CDSCET has reduced the total computation cost by at least 56.46%.

Keywords Wireless body area network · Cross domain heterogeneous · Signcryption · Equality test

1. Introduction

Wireless body area network is an advanced medical branch of wireless sensor network, which can help the doctor to monitor the physical condition of patients, analyze the body data and establish instant communications [1]. Normally, the cloud-assisted WBAN generates and uploads a great deal of data to the medical cloud (MC) [2,3]. However, the data in the MC is suffering many security problems, such as data tampering, eavesdropping, and so on. On the one hand, if any attacker invades into the WBAN system, the patient's private data will be exposed and causes economic losses. On the other hand, if the doctor receives tampered data, it will lead to misjudgment of the patient's disease, which in turn will endanger the life safety of patient. To address this challenge, several data transmission schemes and authentication protocols are proposed [4-6], which improve the security of WBAN.

In order to ensure the security of WBAN data, an effective method is to encrypt or signcrypt the WBAN data and upload it to the MC. However, this situation makes the data cannot be searched. To remove this obstacle, Boneh et al. [7] introduced the public key encryption scheme adopting keyword search (PKE-KS). The PKE-KS scheme makes the ciphertext searchable through the use of keywords.

✉ Ming Luo
lmhappy21@163.com

Yusi Pei
1079986574@qq.com

Minrong Qiu
13576203266@qq.com

1 School of Software, Nanchang University, Nanchang 330000, JiangXi, China

2 GongQing Institute of Science and Technology, Nanchang 330000, JiangXi, China

However, PKE-KS has a drawback that it needs to encrypt the plaintext under the same public key. To address the challenge, Yang et al. [8] designed the public key encryption scheme adopting equality test (PKE-ET). In PKE-ET, different public keys can be used to encrypt different ciphertexts, and the equivalence between them can be learned through the corresponding trapdoors. For the WBAN applications, Ramadan et al. [9] formulated a PKE-ET scheme that achieves low computation cost.

Authentication is vital for PKE-ET, and one of the ways to realize authentication is to use the digital signature. As proposed by Zheng et al. [10], signcryption allows digital signatures and data encryption to be performed at the same time, which greatly improving the efficiency. Subsequently, a signcryption scheme that supports equality test was formulated by Xiong et al. [11]. Besides, WBAN usually consists of different cryptographic systems. Hou et al. [12] proposed a heterogeneous signcryption scheme supporting equality test (HTSC-ET) from PKI to CLC for the Internet of things. Xiong et al. [13] proposed a HTSC-ET scheme from PKI to Identity-based cryptographic system (IBC). However, the existing HTSC-ET schemes use the same cryptographic parameters in different cryptographic systems. Moreover, some of these schemes cannot realize RRA or RKSTKA (RRA means that the adversary cannot obtain the result of equality test by resending the previous ciphertext and corresponding trapdoor to the MC; RKSTKA means that the adversary cannot obtain the plaintext from the ciphertext and the session temporary key). To deal with these problems, a cross domain heterogeneous signcryption scheme supporting equality test with different cryptographic parameters that realize RRA and RKSTKA is required.

1.1. Related works

A PKE-ET scheme for cloud-assisted IOV that realizes temporary delegation was proposed by Li et al. [14]. A PKE-ET scheme that improves efficiency and supports partial authorization was proposed by Lin et al. [15]. Deverajan et al. [16] formulated a PKE-ET scheme towards the IIOT, which uses the Near-Ring. Lin et al. [17] designed a pairing-free PKE-ET scheme with authorization. Recently, some researchers have integrated identity-based cryptographic system with PKE-ET (IBE-ET). An IBE-ET scheme with authorization for mobile applications was formulated by Hassan et al. [18]. An IBE-ET scheme towards the cloud medical service was designed by Xu et al. [19]. The IBE-ET scheme proposed by Xu can be resistant to off-line keyword guessing attacks. Furthermore, a certificateless public key encryption scheme with equality test for IIOT was designed by Elhabob et al. [20] that realizes fine-grained access control.

Alornyo et al. [21] introduced signcryption scheme with equality test into IBC. A latticed-based signcryption scheme with equality test under the standard model was proposed by Le et al. [22]. To apply signcryption and equality test functionality into the heterogeneous environment, Hou et al. [12] proposed an HTSC-ET scheme from PKI environment to CLC environment for the Internet of things applications. Xiong et al. [13] presented an HTSC-ET scheme from PKI environment to IBC environment. In addition, Xiong et al. [23] designed an HTSC-ET scheme from IBC environment to PKI environment, which enables a flexible switch between public key encryption to heterogeneous signcryption. However, as far as the author knows, there is no HTSC-ET scheme that uses different cryptographic parameters in different cryptographic systems.

1.2. Our contribution

The CDSCET is formulated in this paper. The main advantages of CDSCET are as follows:

1. CDSCET achieves cross domain heterogeneous with different cryptographic parameters. However, the existing HTSC-ET schemes such as [12,13,23] use the same cryptographic parameters, which are not suitable for the cross domain heterogeneous WBAN environment.

2. CDSCET not only realizes confidentiality, integrity and authentication but also achieves RRA and RKSTKA. However, the existing HTSC-ET schemes [12,13,23] do not fully realize these security attributes.

3. In the signcryption and unsigncryption phase, CDSCET does not need any pairing operation. Compared with [12,13,23], the total computation cost of CDSCET is reduced by at least 56.46%.

2. Preliminaries

2.1. Bilinear pairing

Let G_1 be an additive cyclic group and G_2 be a multiplicative cyclic group. Suppose that G_1 and G_2 have the same prime order q. Following are the properties of the bilinear pairing $\hat{e}: G_1 \times G_1 \to G_2$:

1. Bilinearity. For any $R, S \in G_1$ and $x, y \in Z_q^*$, $\hat{e}(xR, yS) = \hat{e}(R, S)^{xy}$.

2. Non-degeneracy. There exists an $E \in G_1$ that $\hat{e}(E, E) \neq 1_{G_2}$.

3. Computability. Given any $R, S \in G_1$, $\hat{e}(R, S)$ can be calculated in polynomial time.

2.2. Network model of CDSCET

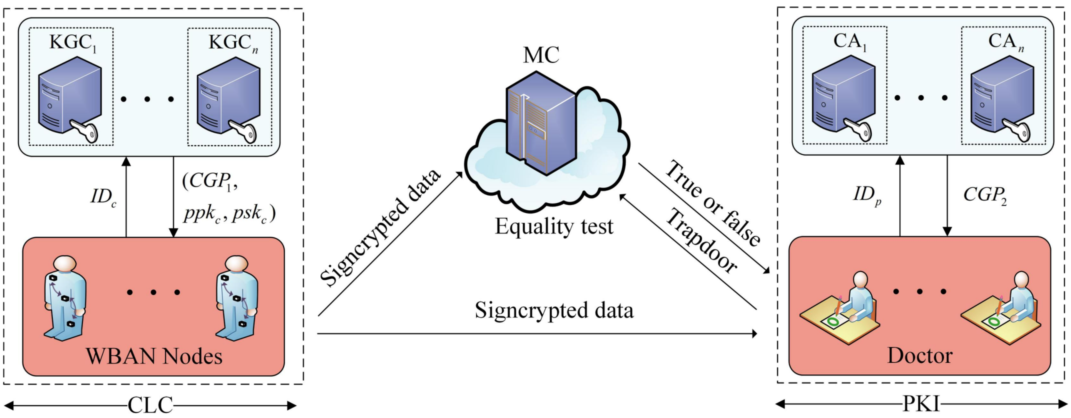

Fig.1 Network model

Fig.1 shows the network model of CDSCET. Five entities make up the network model, including the KGC and WBAN nodes in the CLC environment, CA and doctor in the PKI environment, and MC. Note that every KGC and CA generates different cryptographic parameters. The WBAN nodes collect the body data from the patients and signcrypt it. After that, the signcrypted data is transmitted to the doctor and MC via the wireless networks. When MC receives the corresponding trapdoor from the doctor, it returns true to the doctor if the equality test is passed. Otherwise, MC returns false. The data transmission satisfies confidentiality, integrity and authentication, and is secure against RA and KSTKA.

2.3. Generic model of CDSCET

Setup. KGC generates its secret key a, its public key P_{pub} and outputs the cryptographic parameters CGP_1. Similarly, CA outputs the different cryptographic parameters CGP_2.

CL-PPKG. Given user's identity ID_c in CLC, KGC generates the user's partial public key ppk_c.

CL-PSKG. Given user's identity ID_c in CLC, KGC generates the user's partial private key psk_c.

CL-ASV. Given CGP_1, a user in CLC selects its secret value x_c.

CL-PKG. Given x_c, a user in CLC generates its public key pk_c.

PKI-KGN. Given CGP_2, a user in PKI outputs its public key pk_p and private key x_p.

SC. A sender in CLC executes this algorithm to signcrypt a plaintext m to a receiver in PKI.

USC. The receiver in PKI performs this algorithm to unsigncrypt the ciphertext.

Trapdoor. The receiver in PKI performs this algorithm to generate a trapdoor td.

Test. Given a medical record and a search content with the corresponding trapdoors, this algorithm returns true if the equality test is passed. Otherwise, this algorithm returns false.

2.4. Security model of CDSCET

This section describes the security model of CDSCET. Let B denotes the challenger. Two kinds of adversaries $E_{i(i=1,2)}$ are defined. KGC's master private key cannot be obtained by E_1, but E_1 can replace the public key. Meanwhile, KGC's master private key can be obtained by E_2, but E_2 cannot replace the public key.

Definition 1 If in the following game, each polynomially bounded adversary E_i could win with a negligible advantage, CDSCET owns indistinguishability against adaptive chosen ciphertext attacks (IND-CDSCET-CCA2).

Game 1

Initialization. B executes *Setup* algorithm and sends the cryptographic parameters CGP_1, CGP_2 to E_i.

Phase 1. E_i makes the following queries:

CL-PKG queries. Given an identity ID, B performs *CL-PPKG* and *CL-PKG* algorithm to return E_i the public key (ppk_{ID}, pk_{ID}).

CL-SKG queries. Given an identity ID, B performs *CL-PSKG* and *CL-ASV* algorithm to return the private key psk_{ID} to E_i.

CL-RPK queries. Given a valid public key, the corresponding public key is replaced.

PKI-PKG queries. Given an identity ID, B performs *PKI-KGN* algorithm to return the public key pk_{ID} to E_i.

PKI-SKG queries. Given an identity ID, B performs *PKI-KGN* algorithm to return the private key x_{ID} to E_i.

SC queries. Given the plaintext m and (ID_s, ID_r), B performs *SC* algorithm to return σ to E_i.

USC queries. Given (ID_s, ID_r) and a ciphertext σ , B performs *USC* algorithm and returns the result to E_i .

Trapdoor queries. Given (ID_s, ID_r) and σ , *Trapdoor* algorithm is executed by B and the trapdoor is returned to E_i .

Challenge. E_i sends identities (ID_s^*, ID_r^*) and two plaintexts (m_0, m_1) to B . B chooses $\beta \in \{0,1\}$, performs *SC* algorithm with m_β and returns σ^* to E_i .

Phase 2. E_i makes the same queries as those in Phase 1. However, B rejects if receiving a *PKI-SKG* query of ID_r^* or a *USC* query of $(\sigma^*, ID_s^*, ID_r^*)$.

Guess. E_i outputs β' . If $\beta' = \beta$, E_i wins the game.

Definition 2 If in the following game each polynomially bounded adversary A could win with a negligible advantage, then CDSCET is existentially unforgeable against any adaptive chosen message attacks (EUF-CDSCET-CMA).

Game 2

*Initialization***.** B executes *Setup* algorithm and sends the cryptographic parameters CGP_1, CGP_2 to A .

Probing. The queries are the same as those in Definition 1.

Forgery. A sends identities (ID_s^*, ID_r^*) and σ^* to B . If the following conditions are hold, A wins the game:

(1) The *USC query* of $(\sigma^*, ID_s^*, ID_r^*)$ does not return $\perp$.

(2) The *CL-SKG query* of ID_s^* is not performed.

(3) The *SC query* of σ^* is not performed.

3. CDSCET

This section demonstrates the concrete scheme and its correctness. Fig.2 shows the CDSCET.

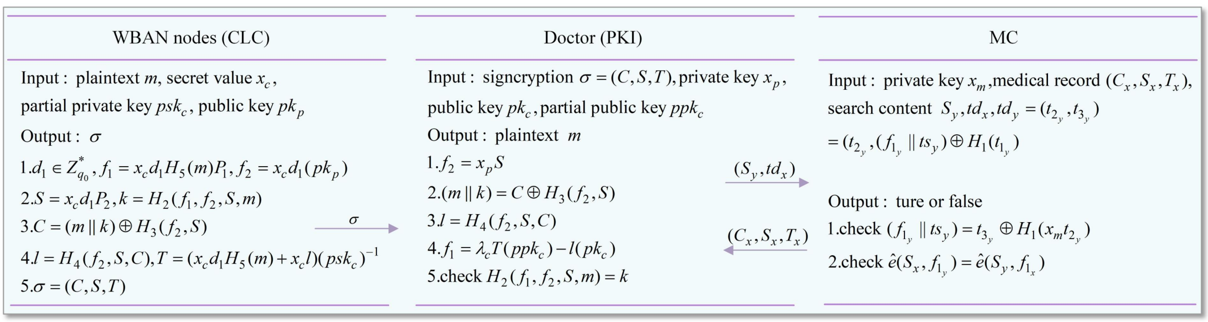

Fig.2 CDSCET

3.1. Construction

Setup. KGC picks G_1, G_2 with the same prime order q_0 . Let P_1 denotes the generator of G_1 . Then KGC sets $\hat{e}: G_1 \times G_1 \to G_2$. Then KGC generates its secret key $a \in Z_{q_0}^*$, its public key $P_{pub} = aP_1$, and defines five hash functions: $H_1: G_1 \to Z_{q_0}^*$, $H_2: G_1^3 \times \{0,1\}^* \to Z_{q_0}^*$, $H_3: G_1^2 \to \{0,1\}^*$,

$H_4 : G_1^{\,2} \times \{0,1\}^* \rightarrow Z_{q_0}^*$ and $H_5 : \{0,1\}^* \rightarrow Z_{q_0}^*$. After that, KGC outputs the cryptographic parameters $CGP_1 = \{G_1, \hat{e}, P_1, P_{pub}, q_0, H_1, H_2, H_3, H_4, H_5, H_6\}$. CA picks G_1' with a prime order q_1 ($q_1 > q_0$ and $|G_1| = |G_1'|$). Let P_2 denotes the generator of G_1'. Then CA generates $x_m \in Z_{q_0}^*, pk_m = x_m P_2$ and sends $\{x_m, pk_m\}$ to MC. Then CA outputs the cryptographic parameters $CGP_2 = \{G_1', P_2, pk_m, q_1\}$.

CL-PPKG. Given the identity ID_c of a user in CLC, KGC selects $b_c \in Z_{q_0}^*$ and computes the user partial public key $ppk_c = b_c P_{pub}$.

CL-PSKG. After performing *CL-PPKG* algorithm, KGC computes $psk_c = ab_c\lambda_c$, where $\lambda_c = H_1(ppk_c)$.

CL-ASV. A user in CLC selects $x_c \in Z_{q_0}^*$ as its secret value.

CL-PKG. After performing *CL-ASV* algorithm, the user calculates $pk_c = x_c P_1$ as another part of its public key.

PKI-KGN. Given the cryptographic parameters CGP_2, a user with identity ID_p in PKI environment selects its private key $x_p \in Z_{q_1}^*$ and computes its public key $pk_p = x_p P_2$.

SC. A sender in CLC signcrypts the plaintext m to a receiver in PKI as follows:

(1) Choose $d_1 \in Z_{q_0}^*$ and compute $f_1 = x_c d_1 H_5(m) P_1, f_2 = x_c d_1 (pk_p)$.

(2) Compute $S = x_c d_1 P_2$, authentication value $k = H_2(f_1, f_2, S, m)$.

(3) Compute $C = (m \| k) \oplus H_3(f_2, S)$ (|| denotes concatenation).

(4) Compute $l = H_4(f_2, S, C)$, $T = (x_c d_1 H_5(m) + x_c l)(psk_c)^{-1}$.

(5) Output $\sigma = (C, S, T)$.

USC. Given $\sigma = (C, S, T)$, the receiver in PKI unsigncrypts the ciphertext. If the ciphertext is valid, this algorithm outputs plaintext m. Otherwise, this algorithm outputs failure symbol $\perp$.

(1) Compute $f_2 = x_p S$.

(2) Compute $(m \| k) = C \oplus H_3(f_2, S)$.

(3) Compute $l = H_4(f_2, S, C)$.

(4) Compute $f_1 = \lambda_c T(ppk_c) - l(pk_c)$.

(5) Check if the authentication value $k = H_2(f_1, f_2, S, m)$ holds. If so, the plaintext m is output. Otherwise, the failure symbol $\perp$ is output.

Trapdoor. In PKI, receiver chooses $d_2 \in Z_{q_1}^*$, computes $t_1 = x_p d_2 pk_m, t_2 = x_p d_2 P_2$. Then it computes the trapdoor $td = (t_2, t_3)$, where $t_3 = (f_1 \| ts) \oplus H_1(t_1)$ and ts is the current timestamp.

Test. Assume that $Z_x = (C_x, S_x, T_x)$ is the medical record in the MC, $Z_y = S_y$ is the search content, and $td_x, td_y = (t_{2_y}, t_{3_y}) = (t_{2_y}, (f_{1_y} \| ts_y) \oplus H_1(t_{1_y})$ are the corresponding trapdoors. To prevent RA, after getting the query (Z_y, td_y) from a user, MC calculates $(f_{1_y} \| ts_y) = t_{3_y} \oplus H_1(x_m t_{2_y})$ and checks if

$ts^{'} - ts_y < \triangle ts$, where $\triangle ts$ is an appropriate period of time and $ts^{'}$ is the current timestamp. If so, MC checks the equation $\hat{e}(S_x, f_{1_y}) = \hat{e}(S_y, f_{1_x})$. If the condition holds, which means the plaintext $m_x = m_y$, then MC returns true. Otherwise, MC returns false.

3.2. Correctness

$$
\begin{aligned}
f_1 &= \lambda_c T(ppk_c) - lpk_c \\
&= \lambda_c (psk_c)^{-1}(d_1 x_c H_5(m) + lx_c) b_c P_{pub} - lx_c P_1 \\
&= \lambda_c (\lambda_c ab_c)^{-1}(d_1 x_c H_5(m) + lx_c) b_c a P_1 - lx_c P_1 \\
&= (ab_c)^{-1} ab_c (d_1 x_c H_5(m) + lx_c) P_1 - lx_c P_1 \\
&= d_1 x_c H_5(m) P_1 + lx_c P_1 - lx_c P_1 \\
&= d_1 x_c H_5(m) P_1
\end{aligned}
$$

and

$$
\begin{aligned}
f_2 &= d_1 x_c PK_p \\
&= x_p d_1 x_c P_2 \\
&= x_p S
\end{aligned}
$$

and

$$
\begin{aligned}
t_1 &= x_p d_2 pk_m \\
&= x_p d_2 x_m P_2 \\
&= x_m t_2
\end{aligned}
$$

and

$$
\begin{aligned}
&\hat{e}(S_x, f_{1_y}) \\
&= \hat{e}(d_{1_x} x_{c_x} P_2, d_{1_y} x_{c_y} H_5(m_y) P_1) \\
&= \hat{e}(P_1, P_2)^{d_{1_x} d_{1_y} x_{c_x} x_{c_y} H_5(m_y)}, \\
&\hat{e}(S_y, f_{1_x}) \\
&= \hat{e}(d_{1_y} x_{c_y} P_2, d_{1_x} x_{c_x} H_5(m_x) P_1) \\
&= \hat{e}(P_1, P_2)^{d_{1_x} d_{1_y} x_{c_x} x_{c_y} H_5(m_x)}
\end{aligned}
$$

4. Security analysis

As demonstrated in this section, CDSCET realizes confidentiality and unforgeability. In addition, CDSCET achieves RRA and RKSTKA.

Definition 1 Decisional Diffie-Hellman Problem (DDHP): Given (P, jP, kP, F) where $j, k \in Z_q^*, P, F \in G_1$, it is difficult to distinguish jkP from F .

Definition 2 Discrete Logarithm Problem (DLP): Given (P, yP) where $y \in Z_q^*, P \in G_1$, it is difficult to compute y .

4.1. Confidentiality

Theorem 1 Assume that DDHP is intractable, in ROM CDSCET is indistinguishable against any IND-CDSCET-CCA2 adversary E_1.

Proof: Assume that the instance of DDHP is (P, jP, kP, F). The process of challenger B uses E_1 to distinguish jkP from F is as follows:

Game 1

Initialization. B performs the *Setup* algorithm, generates the secret key $\{a, x_m, pk_m\}$ and outputs the cryptographic parameters CGP_1, CGP_2.

*Phase*1. B will maintain several lists $L_{i(i=1\sim5)}$ to record $H_{i(i=1\sim5)}$ queries. Meanwhile, B will maintain LK_p and LK_c to record the private key queries of PKI and CLC, respectively.

H_1 *queries*: Given ppk_i as input, B searches L_1 for (ppk_i, λ_i). If the tuple is in L_1, B answers λ_i to E_1. Otherwise, B selects $\lambda_i \in Z_q^*$, inserts (ppk_i, λ_i) to L_1 and returns λ_i to E_1.

H_2 *queries*: Given (f_1, f_2, S_i, m) as input, B searches L_2 for (f_1, f_2, S_i, m, k_i). If the tuple is in L_2, B answers k_i to E_1. Otherwise, B selects $k_i \in Z_q^*$, inserts (f_1, f_2, S_i, m, k_i) to L_2 and returns k_i to E_1.

H_3 *queries*: Given (f_2, S_i) as input, B searches L_3 for (f_2, S_i, h_3). If the tuple is in L_3, B answers h_3 to E_1. Otherwise, B selects $h_3 \in \{0,1\}^*$, inserts (f_2, S_i, h_3) to L_1 and returns h_3 to E_1.

H_4 *queries*: Given (f_2, S_i, C_i) as input, B searches L_4 for (f_2, S_i, C_i, l_i). If the tuple is in L_4, B answers l_i to E_1. Otherwise, B selects $l_i \in Z_q^*$, inserts (f_2, S_i, C_i, l_i) to L_1 and returns l_i to E_1.

H_5 *queries*: Given m_i as input, B searches L_5 for (m_i, h_5). If the tuple is in L_5, B answers h_5 to E_1. Otherwise, B selects $h_5 \in Z_q^*$, inserts (m_i, h_5) to L_1 and returns h_5 to E_1.

CL-PKG queries: Given ID_i as input, B searches LK_c for $(ID_i, x_i, pk_i, psk_i, ppk_i)$ firstly. If the tuple is in LK_c, B returns the public key (pk_i, ppk_i). Otherwise, B picks $x_i, b_i \in Z_q^*$, computes $pk_i = x_i P$, $ppk_i = b_i P_{pub}$, $\lambda_i = H_1(ppk_i)$ and $psk_i = ab_i\lambda_i$, inserts the tuple $(ID_i, x_i, pk_i, psk_i, ppk_i)$ to LK_c and returns the public key (ppk_i, pk_i) to E_1.

CL-SKG queries: Assume that E_1 makes a *CL-PKG* query on ID_i previously, so LK_c contains $(ID_i, x_i, pk_i, psk_i, ppk_i)$. Given ID_i as input, B searches LK_c for $(ID_i, x_i, pk_i, psk_i, ppk_i)$ and returns the private key (x_i, psk_i) to E_1.

CL-RPK queries: Given a valid public key pk_i^*, B updates the tuple $(ID_i, x_i, pk_i, psk_i, ppk_i)$ in LK_c with a new tuple $(ID_i, \perp, pk_i^*, psk_i, ppk_i)$.

PKI-PKG queries: Suppose E_1 makes this query $q_p > 0$ times at most. B picks an identity ID_θ($\theta \in \{1, 2, ...q_p\}$). Given ID_i as input, if $ID_i = ID_\theta$, B sets $x_\theta = \perp, pk_\theta = jP$. If $ID_i \neq ID_\theta$, B

searches pk_i from LK_p. If LK_p does not contain the tuple (ID_i, x_i, pk_i), B picks $x_i \in Z_q^*$ and calculates $pk_i = x_i P$. Finally, B inserts (ID_i, x_i, pk_i) to LK_p and returns the public key pk_i to E_1.

PKI-SKG queries: Assume that E_1 makes a *CL-PKG* query with identity ID_i previously, so LK_p contains (ID_i, x_i, pk_i). B searches LK_p for (ID_i, x_i, pk_i) and returns the private key x_i to E_1.

SC queries: Given (ID_s, ID_r) of sender and receiver, and a plaintext m, B searches (x_c, psk_c, pk_p) from LK_c and LK_p, performs *SC* algorithm and returns $\sigma = (C, S, T)$ to E_1.

USC queries: Given (ID_s, ID_r) of sender and receiver, and $\sigma = (C, S, T)$. B searches $(x_c, ppk_c, x_p, \lambda_c)$ from L_1, LK_c and LK_p, performs *USC* algorithm and returns the result to E_1.

Trapdoor queries: Given ID_r of receiver, and $\sigma = (C, S, T)$. B searches x_p from LK_p, performs *Trapdoor* algorithm and returns the result to E_1.

Challenge. E_1 outputs (ID_s^*, ID_r^*) and two plaintexts (m_0, m_1). Note that the private key of ID_r^* cannot be queried during Phase 1. If $ID_r^* \neq ID_\theta$, B aborts. Otherwise, B picks $\beta \in \{0,1\}$, picks $T^* \in Z_q^*$, computes $S^* = kP$, $f_1^* = (x_s^*)^{-1} S^*$, $f_2^* = F$, $k^* = H_2(f_1^*, f_2^*, S^*, m_\beta)$ and $C^* = (m_\beta \| k^*) \oplus H_3(f_2^*, S^*)$. Finally, B returns $\sigma^* = (C^*, S^*, T^*)$ to E_1.

Phase 2. E_1 makes the same queries as in Phase 1. But B rejects the *PKI-SKG* query of ID_r^* and the *USC* query of $(\sigma^*, ID_s^*, ID_r^*)$.

Guess. E_1 outputs β'. If $\beta' = \beta$, E_1 wins the game, and B can get the solution of DDHP as $F = f_2^* = jkP$. So E_1 can break DDHP with a non-negligible advantage. However, so far there does not exist any efficient algorithm that can solve DDHP. Therefore, CDSCET can achieve confidentiality.

Theorem 2 Assume that DDHP is intractable, in ROM CDSCET is indistinguishable against any IND-CPDSPHS-CCA2 adversary E_2.

Proof: E_2 and B play a game similar to that of Theorem 1, but E_2 is not allowed to make *CL-RPK* or *CL-SKG queries.* If E_2 wants to obtain β, it needs to compute the encryption key f_2^*. Because E_2 does not know the private key x_c of sender, it is also facing DDHP. Therefore, CDSCET is indistinguishable against any IND-CPDSPHS-CCA2 adversary E_2.

4.2. Unforgeability

Theorem 3 Assume that DLP is intractable, in ROM CDSCET is existentially unforgeable against every EUF-CDSCET-CMA adversary A.

Proof: Assume that DLP's instance is (P, yP). Challenger B uses A to get y is as follows:

Game 2

Initialization. B performs the *Setup* algorithm, generates the secret key $\{a, x_m, pk_m\}$ and outputs the cryptographic parameters CGP_1, CGP_2.

Probing. A makes some queries including H_1, H_2, H_3, H_4, *CL-RPK*, *CL-SKG, PKI-PKG* and *PKI-SKG* queries as those in Theorem 1. The *CL-PKG* queries are as follows:

CL-PKG queries: Suppose A makes this query $q_c > 0$ times at most. B picks an identity $ID_\theta(\theta \in \{1,2,...q_c\})$. Given ID_i as input, if $ID_i = ID_\theta$, B sets $x_\theta = \perp$ and $pk_\theta = yP$. If $ID_i \neq ID_\theta$, B searches pk_i from LK_c. If LK_c does not contain the tuple $(ID_i, x_i, pk_i, ppk_i, psk_i)$, B picks $x_i \in Z_q^*$ and computes $pk_i = x_i P$. Finally, B picks $b_i \in Z_q^*$, computes $ppk_i = b_i P_{pub}$, $\lambda_i = H_1(ppk_i)$ and $psk_i = ab_i\lambda_i$, inserts $(ID_i, x_i, pk_i, ppk_i, psk_i)$ to LK_c and returns the public key (pk_i, ppk_i) to A.

Forgery. A outputs (ID_s^*, ID_r^*) of sender and receiver and $\sigma^* = (C^*, S^*, T^*)$. Note that the private key of ID_s^* cannot be queried and σ^* cannot be generated by *SC* query. If $ID_s^* \neq ID_\theta$, B aborts. Otherwise, B computes $f_2^* = x_r^* S^*$ and $l^* = H_4(f_2^*, S^*, C^*)$. Using the forking lemma 12, another valid signcryption $\sigma' = (C', S', T')$ is generated and B can get the answer of DLP just as follows:

$$T^* = (x_c d_1 H_5(m) + yl^*)(psk_\theta)^{-1},$$
$$T' = (x_c d_1 H_5(m) + yl')(psk_\theta)^{-1},$$
$$psk_\theta T^* - l^* y = psk_\theta T' - l' y,$$
$$y = \frac{psk_\theta(T^* - T')}{l^* - l'}$$

Hence, A owns a non-negligible advantage over DLP. Until now however, there hasn't been an efficient algorithm that is able to solve DLP. Therefore, CDSCET can achieve unforgeability.

4.3. RRA

Assume that an adversary intercepts the ciphertext $\sigma = (C, S, T)$ and the trapdoor $td = (t_2, t_3) = (t_2, (f_1 \| ts) \oplus H_1(t_1))$, it submits σ with td to the MC as a RA. If MC lacks a verification of timestamp, the result of equality test will be sent to the adversary. In CDSCET, MC will check the timestamp ts and reject this malicious query. Therefore, CDSCET can realize RRA. However, HHC [12] and XHH [23] cannot realize RRA. In HHC [12], the cloud server directly performs the equality test after receiving the ciphertext C and trapdoor td. Similarly, in XHH [23], the cloud server performs the equality test algorithm without verification.

4.4. RKSTKA

Assume that an adversary gets the temporary key d_1 and the ciphertext $\sigma = (C, S, T)$. The encryption key is $H_3(f_2, S)$, where $f_2 = x_c d_1(pk_p)$. The adversary cannot calculate the encryption key because it cannot calculate the secret value x_c. Therefore, CDSCET can realize RKSTKA. However, HHC [12] XZH [13] and XHH [23] cannot realize RKSTKA. In HHC [12], the encryption key is $H_3(J_1, t_1 PK_{i,1})$, where $J_1 = \hat{e}(P_{pub}, U_{i,1})^{t_1}$. Because $U_{i,1}, PK_{i,1}, P_{pub}$ are public values, if the adversary can get the temporary key t_1, it can compute the encryption key $H_3(J_1, t_1 PK_{i,1})$. The encryption key of XZH [13] is $H_3(r_1)$, where $r_1 = g^{x_1}$. Because g is public, if the adversary can get the temporary key x_1, it can compute the encryption key $H_3(r_1)$. In XHH [23], the encryption key is $H_4(U_2)$, where $U_2 = t^{u_1}$. Because t is public, if the adversary can get the temporary key u_1 , it can compute the encryption key $H_4(U_2)$.

5. Efficiency analysis

In this section, we compare the performance and security of our CDSCET with HHC [12] XZH [13] and XHH [23]. For convenience, Table 1 demonstrates the meaning of different symbols. Besides, the experiment platform is similar to 13: a PC running Windows-10 system, PBC library, 3.60 ghz CPU and 8 gb memory. In addition, Table 2 illustrates the computation cost of different operations.

TABLE 1. Notation

Symbol	Meaning
E	Point exponentiation
A	Point addition
P	Pairing operation
H	Hash function operation
$\|Z_q^*\|$	Element in Z_q^*
$\|G_1\|$	Element in G_1
CL	Length of ciphertext
SK	Length of private key
RRA	Resist Replay attack
RKSTKA	Resist known session temporary key attack
NKEP	No key escrow problem
DCP	Different cryptographic parameters

TABLE 2. Computation cost of different operation.

Operation	E	A	P	H
Time(ms)	0.188	1.229	5.337	0.0008

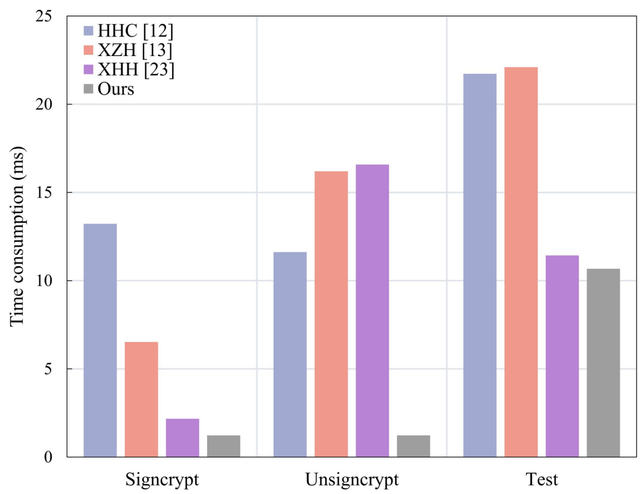

Fig.3 Comparison of computation cost

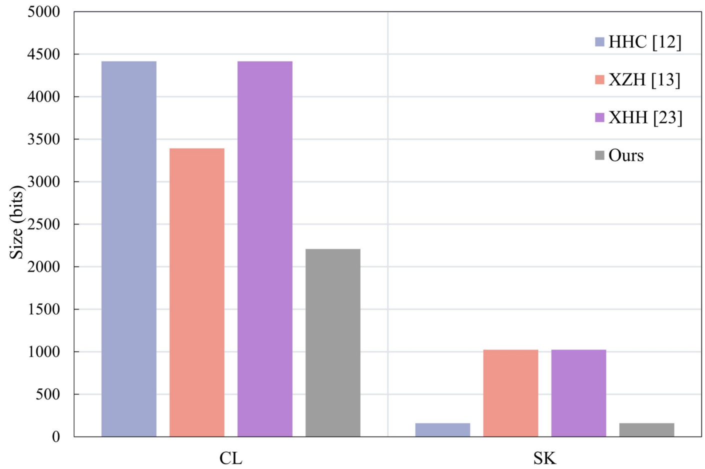

Fig.4 Comparison of communication overhead.

TABLE 3. Comparison of performance.

Scheme	Computation cost			Communication overhead	
	Signcrypt	Unsigncrypt	Equality test	CL	SK
HHC [12]	$A+7E+2P+4H$	$5E+2P+4H$	$2E+4P+2H$	$4\|G_1\|+2\|Z_q^*\|$	$\|Z_q^*\|$
XZH [13]	$5A+2E+5H$	$E+3P+4H$	$4E+4P+2H$	$3\|G_1\|+2\|Z_q^*\|$	$\|G_1\|$
XHH [23]	$A+5E+4H$	$3E+3P+4H$	$4E+2P+2H$	$4\|G_1\|+2\|Z_q^*\|$	$\|G_1\|$
Ours	$A+5H$	$A+3H$	$2P+H$	$2\|G_1\|+\|Z_q^*\|$	$\|Z_q^*\|$

We compare our scheme with [12,13,23] in terms of computation cost and communication overhead in Table 3. Fig.3 demonstrates the computation cost of different schemes. From Fig.3, in the signcryption phase, when compared with [12,13,23], our scheme reduces the computation cost by 90.67%, 43.23% and 81.1%, respectively. In addition, in the unsigncryption phase, our scheme performs better than [12,13,23], which reduces the computation cost by 89.4%, 92.57% and 92.4%, respectively. Moreover, in the equality test phase, compared with [12,13,23] our scheme reduces the computation cost by 50.87%, 6.6% and 51.7%, respectively. From Table 2 and Table 3, the total computation cost of different schemes is shown below:

HHC [12]: $A+14E+8P+10H = 1.229+14\times 0.188+8\times 5.337+10\times 0.0008 = 46.565ms$;

XZH [13]: $5A+7E+7P+11H = 5\times 1.229+7\times 0.188+7\times 5.337+11\times 0.0008 = 44.8288ms$;

XHH [23]: $A+12E+5P+10H = 1.229+12\times 0.188+5\times 5.337+10\times 0.0008 = 30.178ms$;

Ours: $2A+9P+9H = 2\times 1.229+9\times 0.188+9\times 0.0008 = 13.1384ms$;

In conclusion, the total computation cost of our scheme is reduced by at least 56.46% when compared with [12,13,23].

From [13], each element in G_1 is 1024bits and each element in Z_q^* is 160bits. Fig.4 demonstrates the computation overhead of different schemes. From Fig.4, the private key length of our scheme is the same as HHC [12], and is much shorter than XZH [13] and XHH [23]. Besides, from Table 3 we can compute the ciphertext length of different schemes as follows:

HHC [12]: $4|G_1|+2|Z_q^*|=4\times1024+2\times160=4416bits$;

XZH [13]: $3|G_1|+2|Z_q^*|=3\times1024+2\times160=3392bits$;

XHH [23]: $4|G_1|+2|Z_q^*|=4\times1024+2\times160=4416bits$;

Ours: $2|G_1|+|Z_q^*|=2\times1024+160=2208bits$.

In conclusion, the communication overhead of our scheme is reduced by at least 34.9% when compared with [12,13,23].

TABLE 4. Comparison of security.

Scheme	Confidentiality	Integrity	Authentication	RRA	RKSTKA	NKEP	DCP	Environment
HHC [12]	Y	Y	Y	N	N	Y	N	PKI-CLC
XZH [13]	Y	Y	Y	Y	N	N	N	PKI-IBC
XHH [23]	Y	Y	Y	N	N	N	N	IBC-PKI
Ours	Y	Y	Y	Y	Y	Y	Y	CLC-PKI

Table 4 illustrates the comparison of security between different schemes. Let "Y" denotes that the scheme has achieved the corresponding security attribute, and "N" indicates that the attribute is unrealized. From Table 4, compared with HHC [12] and XHH [23], our scheme achieves RRA. Besides, our scheme is the only scheme that realizes RKSTKA when compared with [12,13,23]. The specific analysis of RRA and RKSTKA is described in section 4.3 and 4.4. In addition, our scheme is not affected by the key escrow problem. Because in XZH [13] the user uses IBC system, and in XHH [23] the sensor and user use IBC system, both of them are suffer from the key escrow problem. Moreover, only our scheme uses different cryptographic parameters in different cryptographic systems. In [12,13,23], the sender and receiver use the same cryptographic parameters. Because of their limitations, each security domain cannot independently control its parameters and has to negotiate and share parameters with other domains, which diminishes their practicality.

In conclusion, when compared [12,13,23] our scheme achieves more security attributes and higher efficiency, therefore is more suitable for the cross domain heterogeneous WBAN environment.

6. Conclusion

This paper presents a cross domain heterogeneous signcryption scheme with equality test for WBAN. In our CDSCET, the WBAN node in CLC environment can signcrypt the body data to the doctor in PKI environment. Meanwhile, MC can execute the equality test to compare different medical records through the corresponding trapdoors and return the result to the doctor. In ROM, CDSCET is able to achieve confidentiality and unforgeability under DDHP and DLP. Moreover, CDSCET achieves RRA and RKSTKA. Through the efficiency analysis, when compared to [12,13,23], the total computation cost of CDSCET has reduced by at least 56.46%. Therefore, CDSCET is more suitable for cross domain heterogeneous WBAN environment.

Declarations

Ethical approval and consent to participate

Not applicable.

Human and animal ethics

This article does not contain any studies with human participants or animals performed by any of the authors.

Consent for publication

Not applicable.

Availability of supporting data

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Competing interests

The authors have no competing interests to declare that are relevant to the content of this article.

Funding

This study was funded by the National Natural Science Foundation of China (grant number 61862042) and postgraduate innovation foundation of Nanchang University (No. YC2021-S167).

Authors' contributions

Ming Luo and Yusi Pei wrote the main manuscript text, Minrong Qiu prepared tables 1-4 and figures 1-4. All authors reviewed and approved the final version of the manuscript.

References

1. Cornet, B., Fang, H., & Ngo, H. (2022). An Overview of Wireless Body Area Networks for Mobile Health Applications. *IEEE Network*, *36*(1), 76-82.
2. Ananthi, J. V., & Jose, P. (2021). A Perspective Review of Security Challenges in Body Area Networks for Healthcare Applications. *International Journal of Wireless Information Networks*, *28*(4), 451-466.
3. Azees, M., Vijayakumar, P., & Karuppiah, M. (2021). An efficient anonymous authentication and confidentiality preservation schemes for secure communications in wireless body area networks. *Wireless Networks*, *27*(3), 2119-2130.
4. Cheng, Q., Li, Y., & Shi, W. (2021). A Certificateless Authentication and Key Agreement Scheme for Secure Cloud-assisted Wireless Body Area Network. *Mobile Networks and Applications*, 1-11.
5. Narwal, B., & Mohapatra, A. K. SAMAKA. (2021). Secure and Anonymous Mutual Authentication and Key Agreement Scheme for Wireless Body Area Networks. *Arabian Journal for Science and Engineering*, 1-23.
6. Izza, S., Benssalah, M., & Drouiche, K. (2021). An enhanced scalable and secure RFID

authentication protocol for WBAN within an IoT environment. *Journal of Information Security and Applications*, *58*, 102705.
7. Boneh, D., Di, Crescenzo. G., & Ostrovsky, R. (2004). Public key encryption with keyword search. In *International conference on the theory and applications of cryptographic techniques*, 506-522.
8. Yang, G., Tan, C. H., & Huang, Q. (2010). Probabilistic public key encryption with equality test. In *Cryptographers' track at the RSA conference*, 119-131.
9. Ramadan, M., Liao, Y., & Li, F. (2020). IBEET-RSA: Identity-based encryption with equality test over RSA for wireless body area networks. *Mobile Networks and Applications*, *25*(1), 223-233.
10. Zheng, Y. (1997). Digital signcryption or how to achieve cost (signature & encryption)≪ cost (signature)+ cost (encryption). In *Annual international cryptology conference*, 165-179.
11. Xiong, H., Hou, Y., & Huang, X. (2020). Secure message classification services through identity-based signcryption with equality test towards the Internet of vehicles. *Vehicular Communications*, *26*, 100264.
12. Hou, Y., Huang, X., & Chen, Y. (2021). Heterogeneous Signcryption Scheme Supporting Equality Test from PKI to CLC toward IoT. *Transactions on Emerging Telecommunications Technologies*, *32*(8), e4190.
13. Xiong, H., Zhao, Y., & Hou, Y. (2020). Heterogeneous signcryption with equality test for IIoT environment. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2020.3008955.
14. Li, W., Xia, C., & Wang, C. (2022). Secure and Temporary Access Delegation With Equality Test for Cloud-Assisted IoV. *IEEE Transactions on Intelligent Transportation Systems*. https://doi.org/10.1109/TITS.2022.3174716.
15. Lin, H., Zhao, Z., & Gao, F. (2021). Lightweight Public Key Encryption With Equality Test Supporting Partial Authorization in Cloud Storage. *The Computer Journal*, *64*(8), 1226-1238.
16. Deverajan, G. G., Muthukumaran, V., & Hsu, C. H. (2022). Public key encryption with equality test for Industrial Internet of Things system in cloud computing. *Transactions on Emerging Telecommunications Technologies*, *33*(4), e4202.
17. Lin, X. J., Sun, L., & Qu, H. (2021). Public key encryption supporting equality test and flexible authorization without bilinear pairings. *Computer Communications*, *170*: 190-199.
18. Hassan, A., Elhabob, R., & Eltayieb, N. (2021). An authorized equality test on identity-based cryptosystem for mobile social networking applications. *Transactions on Emerging Telecommunications Technologies*, e4361.
19. Xu, Y., Wang, M., & Zhong, H. (2021). IBEET-AOK: ID-based encryption with equality test against off-line KGAs for cloud medical services. *Frontiers of Computer Science*, *15*(6), 1-3.
20. Elhabob, R., Zhao, Y., & Sella, I. (2020). An efficient certificateless public key cryptography with authorized equality test in IIoT. *Journal of Ambient Intelligence and Humanized Computing*, *11*(3), 1065-1083.
21. Alornyo, S., Mohammed, M. A., & Anibrika, B. S. (2021). ID-Based Plaintext Checkable Signcrypti on with Equality Test in Healthcare Systems. *SN Computer Science*, *2*(1): 1-9.
22. Le, H. Q., Duong, D. H., & Roy, P. S. (2021). Lattice-based signcryption with equality test in standa rd model. *Computer Standards & Interfaces*, *76*: 103515.
23. Xiong, H., Hou, Y., & Huang, X. (2021). Heterogeneous Signcryption Scheme From IBC to PKI Wi th Equality Test for WBAN. *IEEE Systems Journal*. https://doi.org/10.1109/JSYST.2020.3048972.