Journal of Information Hiding and Multimedia Signal Processing ©2016 ISSN 2073-4212
Ubiquitous International Volume **7**, Number **4**, July **2016**

An Efficient Human-Verifiable Key Agreement Scheme with Privacy Preserving with Human Bond Communication for Mobile Devices

Jeng-Shyang Pan

Fuzhou University of International Studies and Trade
Fujian Province, China
No. 28, Yuhuan Road, Changle, Fuzhou City 350202, Fujian Province, China
jspan@cc.kuas.edu.tw

Hongfeng Zhu*

Software College
Shenyang Normal University
No.253, HuangHe Bei Street, HuangGu District, Shenyang, P.C 110034 China
*Corresponding author: zhuhongfeng1978@163.com

Received May, 2016; revised June, 2016

Abstract. *Since the 1990s, chaotic systems have widely used to cryptography which can be used to design kinds of secure protocols, digital signatures, hash functions and so on. And recently, modern communication technology is progressively enabling humans to communicate their information through them with speech (aural) and media (optical) as underpinning essence, even with olfactory, gustatory and tactile (called human bond communication). So there is an intuitive connection among human bond communication, mobile devices and chaotic maps to design a convenient, efficient and high-level secure authenticated key agreement scheme. In this paper, we propose two kinds of optimal authenticated key agreement protocols with chaotic maps for mobile devices in human bond communication: two-party instance and three-party instance. Our proposed protocols' security are mainly based on human-verifiable and chaotic maps. In contrast to the recent literature, our proposed scheme not only cares about security and efficiency, but also provides privacy protection which is a very important property in the modern social network. Finally, we give the security proof and the efficiency analysis of our proposed scheme.*

Keywords: Key agreement; Human bond communication, Human verification, privacy protection, Chaotic maps.

1. **Introduction.**

Wide deployment of mobile devices, such as smart phones equipped with low cost sensors, has already shown great potential in improving the quality of people. Many remote mobile applications, such as mobile game, mobile health, mobile stock and so on, are developing rapidly. But nobody wants to use these mobile applications unless their information and privacy are protected well. So, the common security protection mechanism is the key of mobile Internet user growth. The general security protection mechanism is still mutual authentication key agreement/exchange (MAKA/E) protocol which is used to set up an authenticated and confidential communication channel. The existing authentication protocols adopt passwords [1][4], long secret keys [5], or public key [6] as the proofs of identity. However, most of the above methods are impractical or insecure for this situation. For example, password-based scheme will suffer to guessing attacks (on-line/off-line) easily, and the other two are not good for user experience (impractical). In order to solve above-mentioned problems, human-verifiable authentication protocols [7,8] emerge at the right moment. The key idea of the literatures [7,8] is to provide data integrity via the visual channel. This method does not require preshared keys or preregistered public keys. So, in this paper, based on the literatures [7,8], we put forward an optimal Human-Verifiable key agreement scheme with privacy preserving with Human Bond Communication. Next, we explain two main elements of this paper, Human Bond Communication and Chaotic maps, and give our contributions.

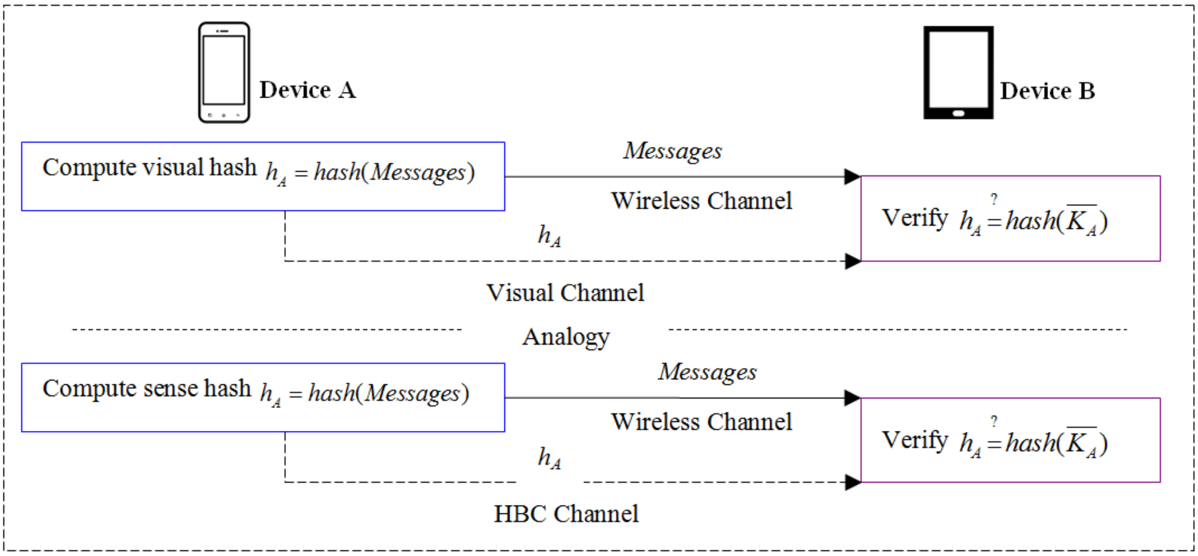

Device A
Device B
Compute visual hash $h_A = hash(Messages)$
Messages
Wireless Channel
h_A
Verify $h_A \overset{?}{=} hash(\overline{K_A})$
Visual Channel
Analogy
Compute sense hash $h_A = hash(Messages)$
Messages
Wireless Channel
h_A
Verify $h_A \overset{?}{=} hash(\overline{K_A})$
HBC Channel

FIGURE 1. SiB protocol and SaB protocol with HBC

(1) Human Bond Communication [9]. Human bond communication is a novel concept that incorporates olfactory, gustatory, and tactile (with the popular senses: optical (media) and auditory (speech)) that will allow more expressive and holistic sensory information exchange through communication techniques for more human sentiment centric communication. We can expand Seeing-is-Believing (SiB) [7] to Senses-are-Believing (SaB) with Human Bond Communication. And based on [8], we change the visual channel to HBC channel (see Fig.1).

(2) Chaotic maps. Unlike digital signature needing the third party for arbitration and many other properties, MAKA/E protocols are only related with the involving participants, so naturally the efficient chaotic cryptosystem is the first candidate. Compared with other cryptosystem systems, a chaotic system has many merits, such as sensitivity to initial arguments, unpredictability, deterministic random-like process and so on. In the past few decades, cryptography systems based on chaos theory have been studied widely [10-19, 23, 24], such as two-party AKA schemes [10], three-party AKE schemes [11], visual authenticated scheme [12], random number generating [13], symmetric encryption [14], asymmetric encryption [15], hash functions [16], digtal signature [17], anonymity scheme [18], Multi-server Environment (Centralized Model) [11], Multiple Servers to Server Architecture (Distributed Model) [19].

(3) Contributions. The two proposed protocols achieves more security goals than the related literature. These security goals include security attribute (privacy protection, authentication, forward secrecy and so on), resistance attribute (Resist impersonation attack, Resist replay attack and so on) and a formal security proof (BAN locig). The

other side, our proposed protocols achieve high-efficiency comparing with the related literature.

The paper is organized as follows: Some preliminaries are given in Section 2. Next, two instances with privacy-protection are described in Section 3. Then, the security analysis and efficiency analysis are given in Section 4 and Section 5. This paper is finally concluded in Section 6.

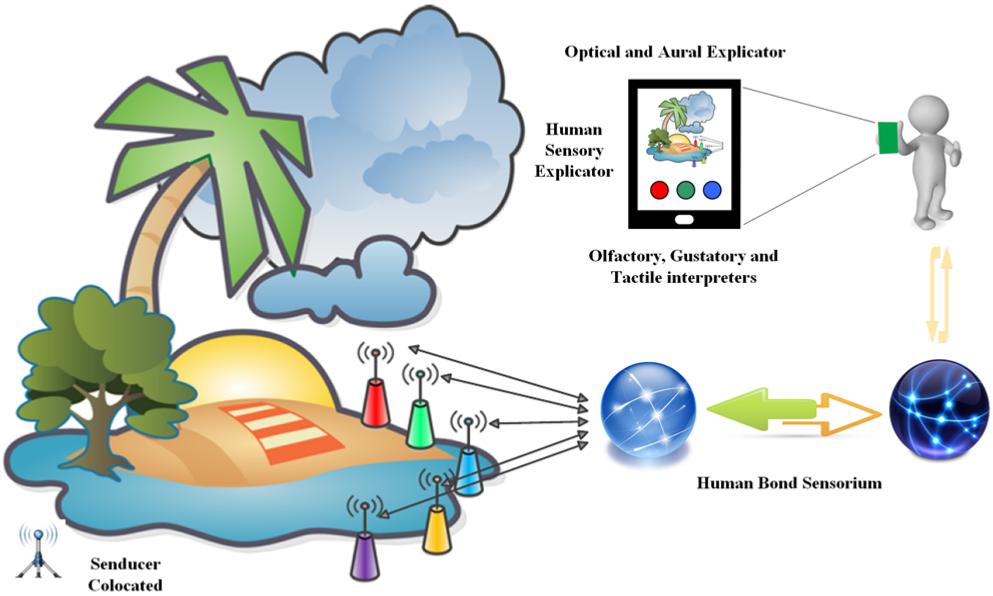

Optical and Aural Explicator
Human Sensory Explicator
Olfactory, Gustatory and Tactile interpreters
Human Bond Sensorium
Senducer Colocated

Figure 2. HBC system architecture

2. Preliminaries.

2.1. Chebyshev chaotic maps. Zhang [20] proved that semi-group property holds for Chebyshev polynomials defined on interval (-,+). The enhanced Chebyshev polynomials are used in the proposed protocol:

$$T_n(x) = (2xT_{n-1}(x) - T_{n-2}(x))(\mathrm{mod} N)$$

where $n \geq 2, x \in (-\infty, +\infty)$ and N is a large prime number.
Obviously

$$T_{rs}(x) = T_r(T_s(x)) = T_s(T_r(x))$$

Definition 1. *(Enhanced Chebyshev polynomials)* The enhanced Chebyshev maps of degree n are defined as:

$$T_n(x) = (2xT_{n-1}(x) - T_{n-2}(x))(\mathrm{mod} p)$$

where $n \geq 2\, x \in (-\infty, +\infty)$, and p is a large prime number.
Obviously,

$$T_{rs}(x) = T_r(T_s(x)) = T_s(T_r(x)) = T_{sr}(x)$$

Definition 2. *(DLP, Discrete Logarithm Problem)* Given an integer a, find the integer r, such that $T_r(x) = a$.

Definition 3. *(CDH, Computational DiffieHellman Problem)* Given an integer x, and the values of $T_r(x), T_s(x)$, what is the value of $T_{rs}(x) =?$

It is widely believed that there is no polynomial time algorithm to solve DLP, CDH with a non-negligible probability.

2.2. **Adversary Model.** All the following protocols should be analyzed in the same adversary model below:

(1) Adversary Λ has full control of the wireless communication channel between communicating parties.

(2) Adversary Λ cannot learn the information in HBC channel.

(3) The (active) adversary Λ can determine the victims identity.

(4) Adversary Λ can learn the previous session key(s).

2.3. **Human Bond Communication [9].** The Human Bond Communication (HBC) architecture mainly consists of three parts (see Fig.2):

(1) senducers that perform sensory transduction of stimuli to electrical signals for further processing;

(2) human bond sensorium (HBS) is the module that collects the information from senducers and processes to make it more human perceivable;

(3) human perceivable transposer (HPT).

The devices that could sample the subject in accordance with the human sensory domain are named here as Sense Transducers or Senducers, they are device equivalent of human senses. The HPT is a device that can transpose the information received from HBS in human perceivable formats. These are proposed devices that can transform the information into the sensory stimuli.

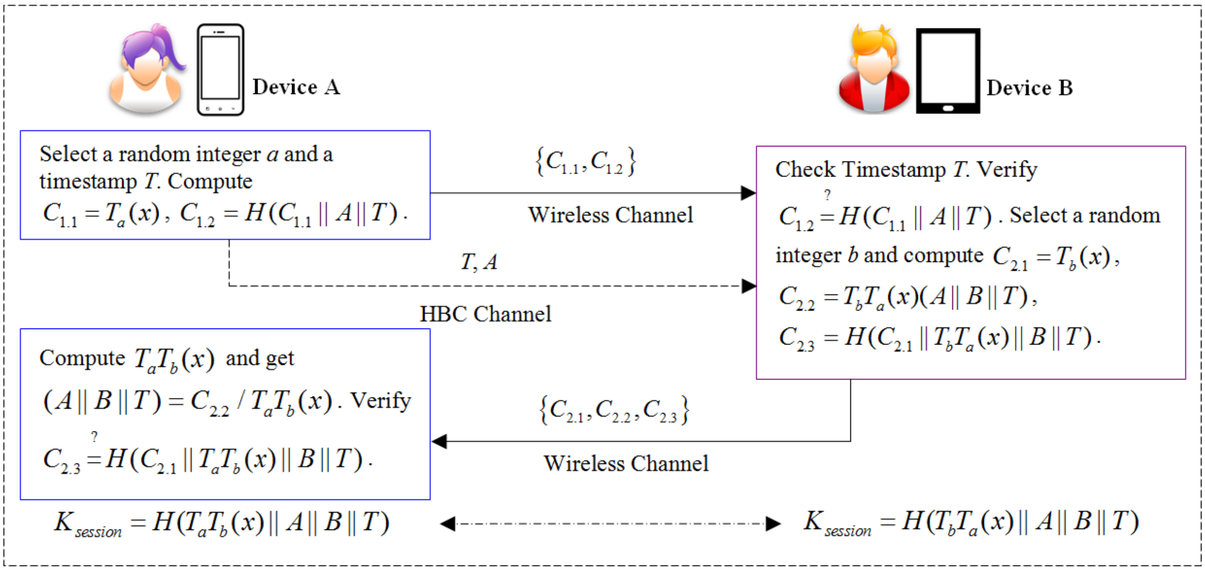

Device A
Device B
Select a random integer a and a timestamp T. Compute $C_{1.1}=T_a(x)$, $C_{1.2}=H(C_{1.1}\|A\|T)$.
$\{C_{1.1}, C_{1.2}\}$
Wireless Channel
Check Timestamp T. Verify $C_{1.2}\overset{?}{=}H(C_{1.1}\|A\|T)$. Select a random integer b and compute $C_{2.1}=T_b(x)$, $C_{2.2}=T_bT_a(x)(A\|B\|T)$, $C_{2.3}=H(C_{2.1}\|T_bT_a(x)\|B\|T)$.
T, A
HBC Channel
Compute $T_aT_b(x)$ and get $(A\|B\|T)=C_{2.2}/T_aT_b(x)$. Verify $C_{2.3}\overset{?}{=}H(C_{2.1}\|T_aT_b(x)\|B\|T)$.
$\{C_{2.1}, C_{2.2}, C_{2.3}\}$
Wireless Channel
$K_{session}=H(T_aT_b(x)\|A\|B\|T)$
$K_{session}=H(T_bT_a(x)\|A\|B\|T)$

FIGURE 3. Two-party instance

2.4. **Basic notations and logical postulates of BAN logic [21].**

3. **The proposed scheme.** The notations in ours used hereafter are shown in Table 3. We assume that all the parties have already some public parameters: H (A secure one-way hash function) and the public parameters of Enhanced Chebyshev polynomials (x, related algorithms). We assume that the HBC channel is secure, and only the human can tell the transfer forms from the five senses. Furthermore, we assume that any party use his own mobile device must be authenticated by his own biometric method.

TABLE 1. Notations of the BAN logic

Symbol	Definition
$P \mid\equiv X$	P believes a statement X.
$\#(X)$	X is fresh.
$P \mid\Rightarrow X$	P has jurisdiction over the statement X.
$P \triangleleft X$	P sees the statement X.
$P \mid\sim X$	P once said the statement X.
(X,Y)	X or Y is one part of the formula (X,Y).
$\langle X\rangle_Y$	X combined with the formula Y.
$\{X\}_Y$	X is encrypted under the key K.
$(X)_Y$	X is chaotic maps-based hash function with the key K.
$P \xleftrightarrow{K} Q$	P and Q use the shared key K to communicate.
$\xrightarrow{K} P$	The public key of P, and the secret key is described by K^{-1}

TABLE 2. Logical postulates of the BAN logic

Symbol	Definition
$P \mid\equiv P \xleftrightarrow{K} Q, P\{X\}_K \Big/ P \mid\equiv Q \mid\sim X$	The message-meaning rule (R_1)
$P \mid\equiv \#(X) \Big/ P \mid\equiv \#(X,Y)$	The freshness-conjuncatenation rule (R_2)
$P \mid\equiv \#(X), P \mid\equiv Q \mid\sim X \Big/ P \mid\equiv Q \mid\equiv X$	The nonce-verification rule (R_3)
$P \mid\equiv Q \mid\Rightarrow X, P \mid\equiv Q \mid\equiv X \Big/ P \mid\equiv X$	The jurisdiction rule (R_4)
$P \mid\equiv Q \mid\equiv (X,Y) \Big/ P \mid\equiv Q \mid\equiv X$	The belief rules (R_5)
Remark: Molecule can deduce denominator for above formulas.	

TABLE 3. Notations

Symbol	Definition
A, B, C	The identities of the users
A, B, C	The identities of the users' devices
a, b, c	Random numbers
$(x, T_k(x))$	Public key based on Chebyshev chaotic maps for the server
k	Secret key based on Chebyshev chaotic maps for the server
H	A secure one-way hash function
$C_{i.j}$	The exchanging messages or functions
T	Timestamp
$\Vert$	Concatenation operation
$\overset{?}{=}$	Whether both sides of a equation are equal?

3.1. **Two-party instance.** Fig.3 illustrates the user registration phase.

(1). Device A Device B: $\{C_{1.1}, C_{1.2}\}$ with wireless channel; $\{T, A\}$ with HBC channel If Alice wishes to consult some personal issues establish with Bob, she will use her device **A** to choose a random integer number , a timestamp T and compute $C_{1.1} = T_a(x)$, $C_{1.2} = H(C_{1.1}||A||T)$. And at the same time, the device encodes T, A into one kinds of human bond, such as a visual code can be displayed on screen, or sound wave can be played on screen and so on. Finally, **A** sends $\{C_{1.1}, C_{1.2}\}$ with wireless channel and $\{T, A\}$ with HBC channel to **B**.

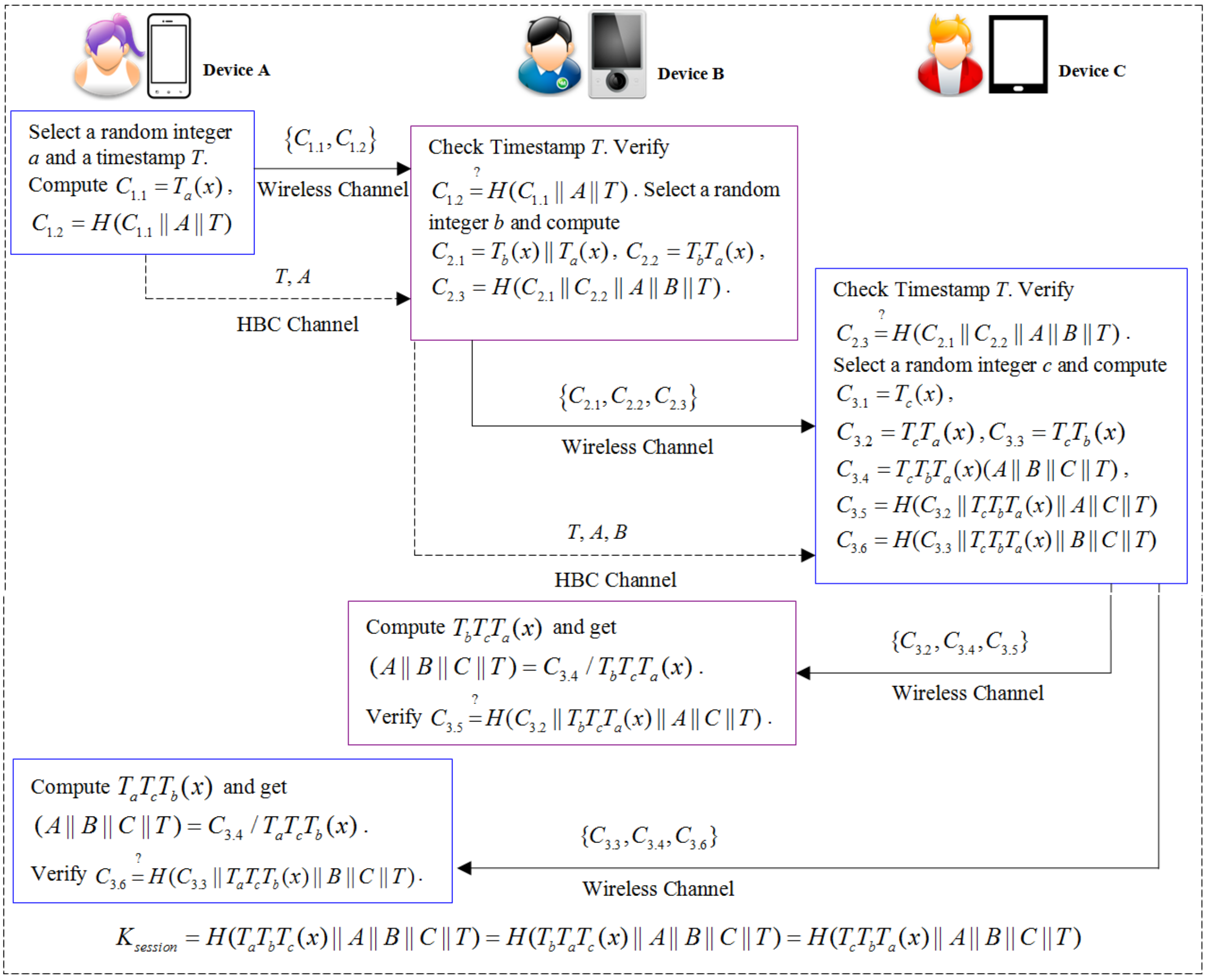

Device A
Device B
Device C
Select a random integer a and a timestamp T. Compute $C_{1.1} = T_a(x)$, $C_{1.2} = H(C_{1.1} || A || T)$
$\{C_{1.1}, C_{1.2}\}$
Wireless Channel
T, A
HBC Channel
Check Timestamp T. Verify $C_{1.2} \overset{?}{=} H(C_{1.1} || A || T)$. Select a random integer b and compute $C_{2.1} = T_b(x) || T_a(x)$, $C_{2.2} = T_bT_a(x)$, $C_{2.3} = H(C_{2.1} || C_{2.2} || A || B || T)$.
$\{C_{2.1}, C_{2.2}, C_{2.3}\}$
Wireless Channel
T, A, B
HBC Channel
Check Timestamp T. Verify $C_{2.3} \overset{?}{=} H(C_{2.1} || C_{2.2} || A || B || T)$. Select a random integer c and compute $C_{3.1} = T_c(x)$, $C_{3.2} = T_cT_a(x)$, $C_{3.3} = T_cT_b(x)$ $C_{3.4} = T_cT_bT_a(x)(A || B || C || T)$, $C_{3.5} = H(C_{3.2} || T_cT_bT_a(x) || A || C || T)$ $C_{3.6} = H(C_{3.3} || T_cT_bT_a(x) || B || C || T)$
$\{C_{3.2}, C_{3.4}, C_{3.5}\}$
Wireless Channel
Compute $T_bT_cT_a(x)$ and get $(A || B || C || T) = C_{3.4} / T_bT_cT_a(x)$. Verify $C_{3.5} \overset{?}{=} H(C_{3.2} || T_bT_cT_a(x) || A || C || T)$.
$\{C_{3.3}, C_{3.4}, C_{3.6}\}$
Wireless Channel
Compute $T_aT_cT_b(x)$ and get $(A || B || C || T) = C_{3.4} / T_aT_cT_b(x)$. Verify $C_{3.6} \overset{?}{=} H(C_{3.3} || T_aT_cT_b(x) || B || C || T)$.
$K_{session} = H(T_aT_bT_c(x) || A || B || C || T) = H(T_bT_aT_c(x) || A || B || C || T) = H(T_cT_bT_a(x) || A || B || C || T)$

FIGURE 4. Three-party instance

(2) Device B Device A: $\{C_{2.1}, C_{2.2}, C_{2.3}\}$ with wireless channel Upon receiving $\{C_{1.1}, C_{1.2}\}$ and $\{T, A\}$ from Alice, Bob firstly confirms the $\{T, A\}$ by his a kind of sensory features and does corresponding actions. After that, based on Bob's actions and $\{C_{1.1}, C_{1.2}\}$, Bob's device B will firstly check timestamp T. Then, B computes $H(C_{1.1}||A||T)$ and verifies $H(C_{1.1}||A||T) \overset{?}{=} C_{1.2}$. If the above equation holds, that means Alice is a legal user, or B will abort this process. After authenticating Alice, B chooses a random and computes $C_{2.1} = T_b(x)$, $C_{2.2} = T_bT_a(x)(A||B||T)$, $C_{2.3} = H(C_{2.1}||T_bT_a(x)||B||T)$ and $K_{session} = H(T_bT_a(x)||A||B||T)$. Finally B sends $\{C_{2.1}, C_{2.2}, C_{2.3}\}$ to A with wireless channel.

(3) After receiving the message $\{C_{2.1}, C_{2.2}, C_{2.3}\}$, **A** computes $T_aT_b(x)$ and gets $(A||B||T) = C_{2.2}/T_aT_b(x)$.

Then **A** computes $H(C_{2.1}||T_aT_b(x)||B||T)$ and verifies $C_{2.3}\overset{?}{=}H(C_{2.1}||T_aT_b(x)||B||T)$. If the above equation holds, **A** will computes the session key $K_{session} = H(T_aT_b(x)||A||B||T)$ locally. Otherwise **A** will abort this process.

3.2. **Three-party instance.** This concrete process is presented in the following Fig.4.

(1) Device A Device B: $\{C_{1.1}, C_{1.2}\}$ with wireless channel; $\{T, A\}$ with HBC channel If Alice wishes to consult some personal issues establish with Bob and Cook, she will use her device **A** to choose a random integer number , a timestamp T and compute $C_{1.1} = T_a(x)$, $C_{1.2} = H(C_{1.1}||A||T)$. And at the same time, the device encodes $\{T, A\}$ into one kinds of human bond, such as a visual code can be displayed on screen, or sound wave can be played on screen and so on. Finally, **A** sends $\{C_{1.1}, C_{1.2}\}$ with wireless channel and $\{T, A\}$ with HBC channel to **B**.

(2) Device B Device C: $\{C_{2.1}, C_{2.2}, C_{2.3}\}$ with wireless channel; $\{T, A, B\}$ with HBC channel Upon receiving $\{C_{1.1}, C_{1.2}\}$ and $\{T, A\}$ from Alice, Bob firstly confirms the $\{T, A\}$ by his a kind of sensory features and does corresponding actions. After that, based on Bob's actions and $\{C_{1.1}, C_{1.2}\}$, Bob's device B will firstly check timestamp T. Then, **B** computes $H(C_{1.1}||A||T)$ and verifies $H(C_{1.1}||A||T)\overset{?}{=}C_{1.2}$. If the above equation holds, that means Alice is a legal user, or **B** will abort this process. After authenticating Alice, **B** chooses a random b and computes $C_{2.1} = T_b(x)||T_a(x)$, $C_{2.2} = T_bT_a(x)$ and $C_{2.3} = H(C_{2.1}||C_{2.2}||A||B||T)$. Finally **B** sends $\{C_{2.1}, C_{2.2}, C_{2.3}\}$ with wireless channel and $\{T, A, B\}$ with HBC channel to **C**.

(3) Device C Device B: $\{C_{2.1}, C_{2.2}, C_{2.3}\}$ with wireless channel Device **C** Device **A**: $\{C_{2.1}, C_{2.2}, C_{2.3}\}$ with wireless channel Upon receiving $\{C_{2.1}, C_{2.2}, C_{2.3}\}$ and $\{T, A, B\}$ from Bob, Cook firstly confirms the $\{T, A, B\}$ by his a kind of sensory features and does corresponding actions. After that, based on Cook's actions and $\{C_{2.1}, C_{2.2}, C_{2.3}\}$, Cook's device **C** will firstly check timestamp T. Then, **C** computes $H(C_{2.1}||C_{2.2}||A||B||T)$ and verifies $H(C_{2.1}||C_{2.2}||A||B||T)\overset{?}{=}C_{2.3}$. If the above equation holds, that means Bob is a legal user, or **C** will abort this process. After authenticating Bob, **C** chooses a random c and computes $C_{3.1} = T_c(x)$, $C_{3.2} = T_cT_a(x)$, $C_{3.3} = T_cT_b(x)$, $C_{3.4} = T_cT_bT_a(x)(A||B||C||T)$, $C_{3.5} = H(C_{3.2}||T_cT_bT_a(x)||A||C||T)$ and $C_{3.6} = H(C_{3.3}||T_cT_bT_a(x)||B||C||T)$. Next, **C** sends $\{C_{3.2}, C_{3.4}, C_{3.5}\}$ with wireless channel to **B** and sends $\{C_{3.3}, C_{3.4}, C_{3.6}\}$ with wireless channel to **A**. Finally, **C** computes the session key $K_{session} = H(T_cT_bT_a(x)||A||B||C||T)$ locally.

(4) After receiving the message $\{C_{3.2}, C_{3.4}, C_{3.5}\}$, **B** computes $T_bT_cT_a(x)$ and get $(A||B||C||T) = C_{3.4}/T_bT_cT_a(x)$. Then **B** computes $H(C_{3.2}||T_bT_cT_a(x)||A||C||T)$ and verifies $H(C_{3.2}||T_bT_cT_a(x)||A||C||T)\overset{?}{=}C_{3.5}$. If the above equation holds, **B** will computes the session key $K_{session} = H(T_bT_aT_c(x)||A||B||C||T)$ locally.

(5) After receiving the message $\{C_{3.3}, C_{3.4}, C_{3.6}\}$, **A** computes $T_aT_cT_b(x)$ and get $(A||B||C||T) = C_{3.4}/T_aT_cT_b(x)$. Then **A** computes $H(C_{3.3}||T_aT_cT_b(x)||B||C||T)$ and verifies $H(C_{3.3}||T_aT_cT_b(x)||B||C||T)\overset{?}{=}C_{3.6}$. If the above equation holds, **A** will computes the session key $K_{session} = H(T_aT_bT_c(x)||A||B||C||T)$ locally.

At last, all the parties will share the session key to set up a secure channel: $K_{session} = H(T_aT_bT_c(x)||A||B||C||T) = H(T_bT_aT_c(x)||A||B||C||T) = H(T_cT_bT_a(x)||A||B||C||T)$.

Remark: *N-party instance.* This scenario is not the common case. And then, if the number N increases bigger and bigger, the N-party instance will be impractical further. Because more people involved and number of the human-verifiable will be more which lead to the bad User Experience. But there are still some methods can be adopted [8].

Simulation 1 BAN logic of two-party instance

Goals: Goal1. $A|\equiv(A\xleftrightarrow{K_{session}}B)$; Goal2. $A|\equiv B|\equiv(A\xleftrightarrow{K_{session}}B)$;
Goal3. $B\equiv(B\xleftrightarrow{K_{session}}A)$; Goal4. $B|\equiv A|\equiv(B\xleftrightarrow{K_{session}}A)$;

Idealized forms of two-party instance:

(A$\rightarrow$B) $C_1: T_a(x),(T_a(x)\|A\|T)$;

B$\rightarrow$A) $C_2: T_b(x),T_bT_a(x)A\|B\|T,(T_b(x)\|T_bT_a(x)\|B\|T)$.

Initial states: ($P_1: A,B|\equiv A\xleftrightarrow{A,T}B$, HBC channel), $P_2: A|\equiv\#(a),P_3: B|\equiv\#(b)$

1: **For** C_1**:** According to the ciphertext C_1 and P_1,P_2 and attributes of chaotic maps, and relating with R_1, we could get: $S_1: B|\equiv A|\sim C_1$.

2: Based on the initial assumptions P_1,P_2, and relating with R_2, we could get: $S_2: B|\equiv\#C_1$.

3: Combining S_1,S_2,P_1,P_2,R_3 and attributes of chaotic maps, we could get: $S_3: B|\equiv\#T_a(x),(T_a(x)\|A\|T)$.

4: Based on R_5, we take apart S_3 and get: $S_4: B|\equiv\#T_a(x),S_5: B|\equiv\#(T_a(x)\|A\|T)$.

5: Combining P_1,S_5 and attributes of chaotic maps with a secure hash function, we can verify that the message C_1 is fresh and comes from Alice exactly.

6: **For** C_2**:** According to the ciphertext C_2 and P_1,P_3 and attributes of chaotic maps, and relating with R_1, we could get: $S_6: A|\equiv B|\sim C_2$.

7: Based on the initial assumptions P_1,P_3, and relating with R_2, we could get: $S_7: A|\equiv\#C_2$.

8: Combining S_6,S_7,P_1,P_3,R_3 and attributes of chaotic maps, we could get: $S_8: A|\equiv\#T_b(x),T_bT_a(x)A\|B\|T,(T_b(x)\|T_bT_a(x)\|B\|T)$.

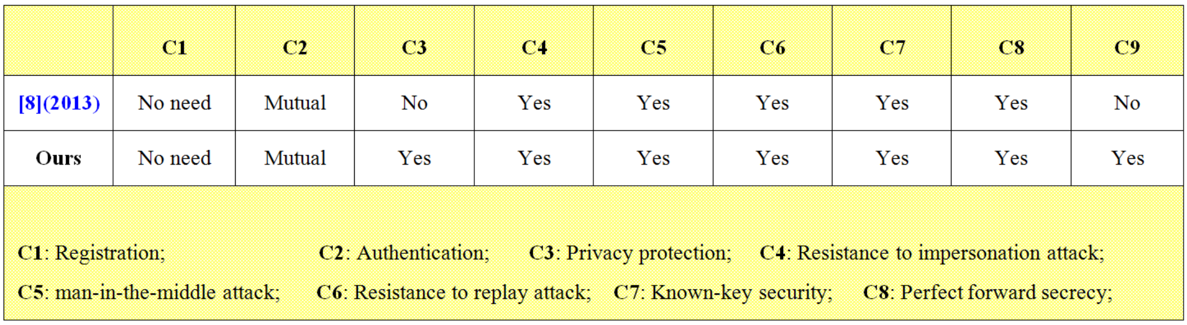
9: Based on R_5, we take apart S_8 and get: $S_9: A|\equiv\#T_b(x)$, $S_{10}: A|\equiv\#T_bT_a(x)A\|B\|T$, $S_{11}: A|\equiv\#(T_b(x)\|T_bT_a(x)\|B\|T)$.

10: Combining P_1,P_2,S_{10} and attributes of chaotic maps, we can get the fresh and privacy protection about identity of Bob.

11: Combining P_1,P_3,S_{11} and attributes of secure chaotic maps-based hash function, we can verify that the message C_2 comes from Bob exactly.

12: **Whole combination:** Since Alice and Bob communicate to each other just now, they confirm the other is on-line. Moreover, since Bob can get $\{T,A\}$ from the HBC channel securely, and based on S_4,S_5,R_4 with chaotic maps problems, and this shows that that Bob could get the session key $K_{session}=H(T_bT_a(x)\|A\|B\|T)$ and Goal3. $B\equiv(B\xleftrightarrow{K_{session}}A)$; Goal4. $B|\equiv A|\equiv(B\xleftrightarrow{K_{session}}A)$. At the other side, since Server can get ID_A from the $T_bT_a(x)A\|B\|T$ with her own secret random number a, and based on S_9,S_{11},R_4 with chaotic maps problems, and this shows that that the server could get the session key $K_{session}=H(T_aT_b(x)\|A\|B\|T)$ and $A|\equiv(A\xleftrightarrow{K_{session}}B)$;Goal2. $A|\equiv B|\equiv(A\xleftrightarrow{K_{session}}B)$.

Table 4. Security Comparison



	C1	C2	C3	C4	C5	C6	C7	C8	C9
[8](2013)	No need	Mutual	No	Yes	Yes	Yes	Yes	Yes	No
Ours	No need	Mutual	Yes	Yes	Yes	Yes	Yes	Yes	Yes

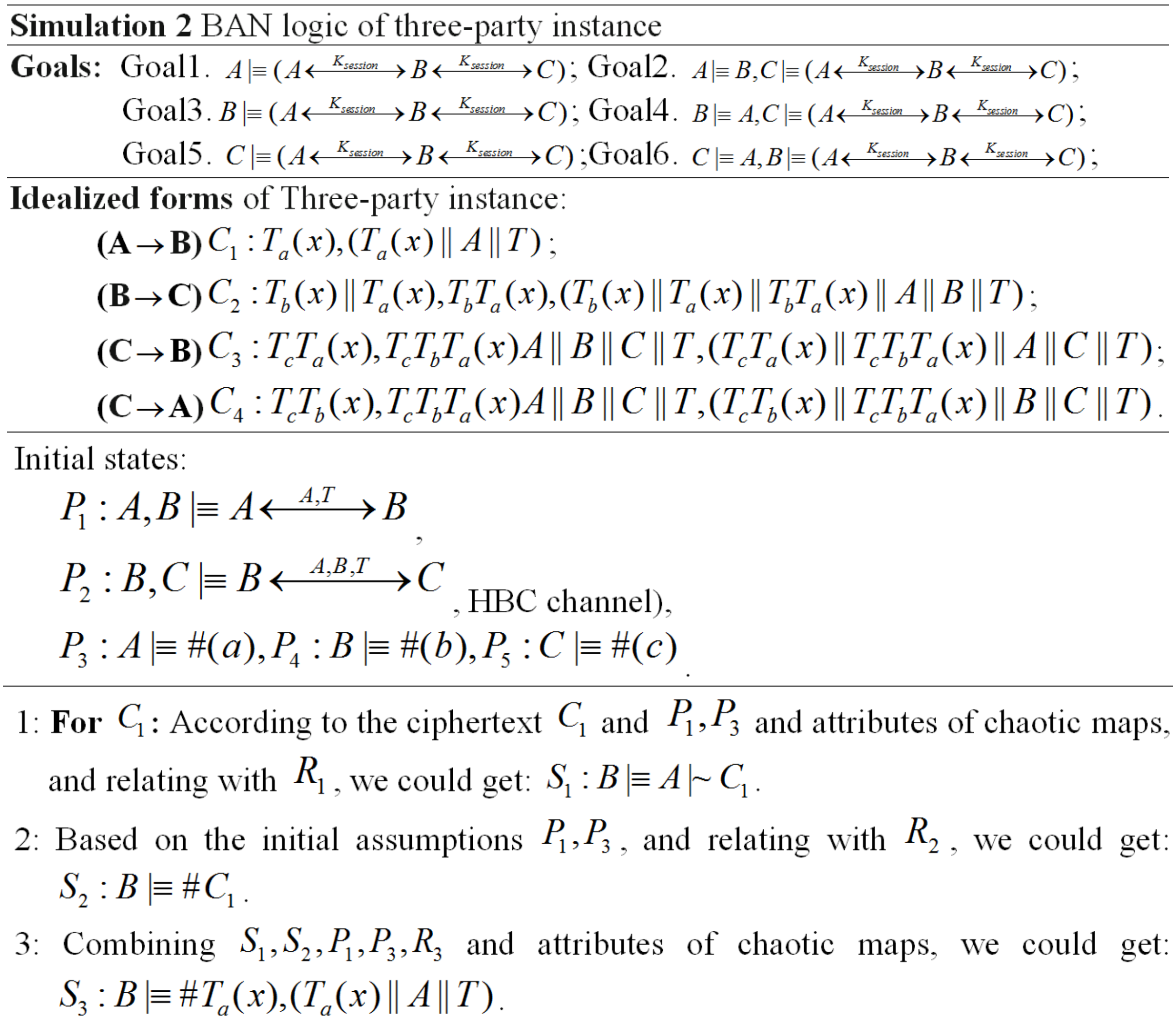
C1: Registration; **C2**: Authentication; **C3**: Privacy protection; **C4**: Resistance to impersonation attack;
C5: man-in-the-middle attack; **C6**: Resistance to replay attack; **C7**: Known-key security; **C8**: Perfect forward secrecy;

4. Security Analysis.

4.1. Security proof based on the BAN logic [21].

According to analytic procedures of BAN logic and chaotic maps, the processes of our two-party and three-party instances are described in:

Simulation 1 and **Simulation 2**.



Simulation 2 BAN logic of three-party instance

Goals: Goal1. $A|\equiv(A\xleftrightarrow{K_{session}}B\xleftrightarrow{K_{session}}C)$; Goal2. $A|\equiv B,C|\equiv(A\xleftrightarrow{K_{session}}B\xleftrightarrow{K_{session}}C)$;
Goal3. $B|\equiv(A\xleftrightarrow{K_{session}}B\xleftrightarrow{K_{session}}C)$; Goal4. $B|\equiv A,C|\equiv(A\xleftrightarrow{K_{session}}B\xleftrightarrow{K_{session}}C)$;
Goal5. $C|\equiv(A\xleftrightarrow{K_{session}}B\xleftrightarrow{K_{session}}C)$;Goal6. $C|\equiv A,B|\equiv(A\xleftrightarrow{K_{session}}B\xleftrightarrow{K_{session}}C)$;

Idealized forms of Three-party instance:

(A→B) $C_1: T_a(x),(T_a(x)\|A\|T)$;

(B→C) $C_2: T_b(x)\|T_a(x),T_bT_a(x),(T_b(x)\|T_a(x)\|T_bT_a(x)\|A\|B\|T)$;

(C→B) $C_3: T_cT_a(x),T_cT_bT_a(x)A\|B\|C\|T,(T_cT_a(x)\|T_cT_bT_a(x)\|A\|C\|T)$;

(C→A) $C_4: T_cT_b(x),T_cT_bT_a(x)A\|B\|C\|T,(T_cT_b(x)\|T_cT_bT_a(x)\|B\|C\|T)$.

Initial states:

$P_1: A,B|\equiv A\xleftrightarrow{A,T}B$,

$P_2: B,C|\equiv B\xleftrightarrow{A,B,T}C$, HBC channel),

$P_3: A|\equiv\#(a),P_4: B|\equiv\#(b),P_5: C|\equiv\#(c)$.

1: **For** C_1: According to the ciphertext C_1 and P_1,P_3 and attributes of chaotic maps, and relating with R_1, we could get: $S_1: B|\equiv A|\sim C_1$.

2: Based on the initial assumptions P_1,P_3, and relating with R_2, we could get: $S_2: B|\equiv\#C_1$.

3: Combining S_1,S_2,P_1,P_3,R_3 and attributes of chaotic maps, we could get: $S_3: B|\equiv\#T_a(x),(T_a(x)\|A\|T)$.

4: Based on R_5, we take apart S_3 and get: $S_4 : B |\equiv \#T_a(x), S_5 : B |\equiv \#(T_a(x) \| A \| T)$.

5: Combining P_1, S_5 and attributes of a secure chaotic maps-based hash function, we can verify that the message C_1 comes from Alice exactly.

6: **For** C_2**:** According to the ciphertext C_2 and P_2, P_4 and attributes of chaotic maps, and relating with R_1, we could get: $S_6 : C |\equiv B |\sim C_2$.

7: Based on the initial assumptions P_2, P_4, and relating with R_2, we could get: $S_7 : C |\equiv \#C_2$.

8: Combining S_6, S_7, P_2, P_4, R_3 and attributes of chaotic maps, we could get: $S_8 : C |\equiv \#T_b(x) \| T_a(x), T_bT_a(x), (T_b(x) \| T_a(x) \| T_bT_a(x) \| A \| B \| T)$.

9: Based on R_5, we take apart S_8 and get: $S_9 : C |\equiv \#T_b(x) \| T_a(x)$, $S_{10} : C |\equiv \#T_bT_a(x)$, $S_{11} : C |\equiv \#(T_b(x) \| T_a(x) \| T_bT_a(x) \| A \| B \| T)$.

10: Combining P_2, P_4, S_{11} and attributes of a secure chaotic maps-based hash function, we can verify that the message C_2 comes from Bob exactly.

11: **For** C_3**:** According to the ciphertext C_3 and P_2, P_5 and attributes of chaotic maps, and relating with R_1, we could get: $S_{12} : B |\equiv C |\sim C_3$.

12: Based on the initial assumptions P_2, P_5, and relating with R_2, we could get: $S_{13} : B |\equiv \#C_3$.

13: Combining $S_{12}, S_{13}, P_2, P_5, R_3$ and attributes of chaotic maps, we could get: $S_{14} : B |\equiv \#T_cT_a(x), T_cT_bT_a(x)A \| B \| C \| T, (T_cT_a(x) \| T_cT_bT_a(x) \| A \| C \| T)$.

14: Based on R_5, we take apart S_{14} and get: $S_{15} : B |\equiv \#T_cT_a(x)$, $S_{16} : B |\equiv \#T_cT_bT_a(x)A \| B \| C \| T$, $S_{17} : B |\equiv \#(T_cT_a(x) \| T_cT_bT_a(x) \| A \| C \| T)$.

15: Combining P_2, P_5, S_{16} and attributes of chaotic maps, we can get the fresh and privacy protection about identities of Bob and Cook.

16: Combining P_2, P_5, S_{17} and attributes of a secure chaotic maps-based hash function, we can verify that the message C_3 comes from Cook exactly.

17: **For** C_4**:** According to the ciphertext C_4 and P_1, P_2, P_5 and attributes of chaotic maps, and relating with R_1, we could get: $S_{18} : A |\equiv C |\sim C_4$.

18: Based on the initial assumptions P_1, P_2, P_5, and relating with R_2, we could get: $S_{19} : A \mid\equiv \# C_4$.

19: Combining $S_{18}, S_{19}, P_1, P_2, P_5, R_3$ and attributes of chaotic maps, we could get: $S_{20} : A \mid\equiv \# T_c T_b(x), T_c T_b T_a(x) A \| B \| C \| T, (T_c T_b(x) \| T_c T_b T_a(x) \| B \| C \| T)$.

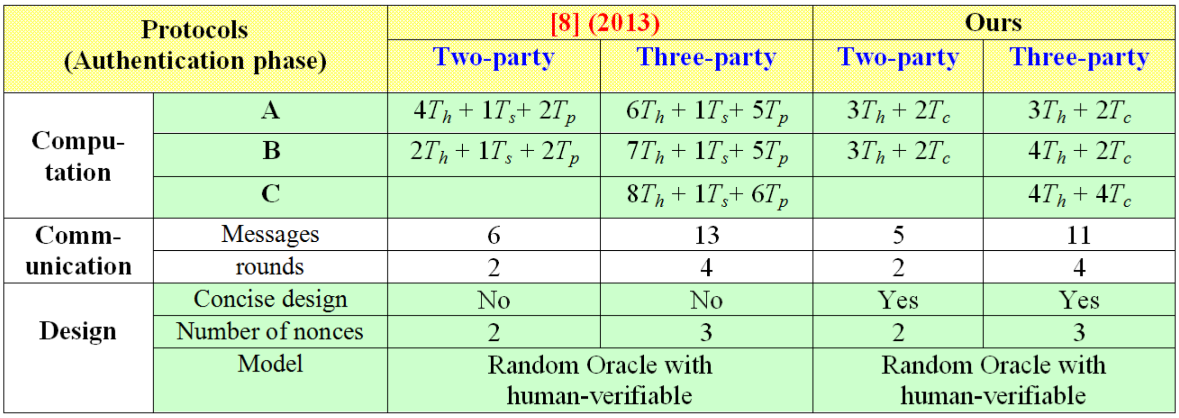
20: Based on R_5, we take apart S_{20} and get: $S_{21} : A \mid\equiv \# T_c T_b(x)$, $S_{22} : A \mid\equiv \# T_c T_b T_a(x) A \| B \| C \| T$, $S_{23} : A \mid\equiv \#(T_c T_b(x) \| T_c T_b T_a(x) \| B \| C \| T)$.

21: Combining P_1, P_2, P_5, S_{22} and attributes of chaotic maps, we can get the fresh and privacy protection about identities of Bob and Cook.

22: Combining P_1, P_2, P_5, S_{23} and attributes of a secure hash function, we can verify that the message C_4 comes from Cook exactly.

23: **Whole combination:** Since Alice, Bob and Cook communicate to each other just now, they confirm the other is on-line. Moreover, based on $P_1, P_2, S_5, S_{11}, S_{17}, S_{23}, R_4$ with chaotic maps problems and a secure chaotic maps-based hash function, and this shows that Alice, Bob and Cook could get the session key $K_{session} = H(T_a T_b T_c(x) \| A \| B \| C \| T) = H(T_b T_a T_c(x) \| A \| B \| C \| T) = H(T_c T_b T_a(x) \| A \| B \| C \| T)$ and the Goals(1-6). □

Table 5. Comparisons between our proposed schemes and the related literatures

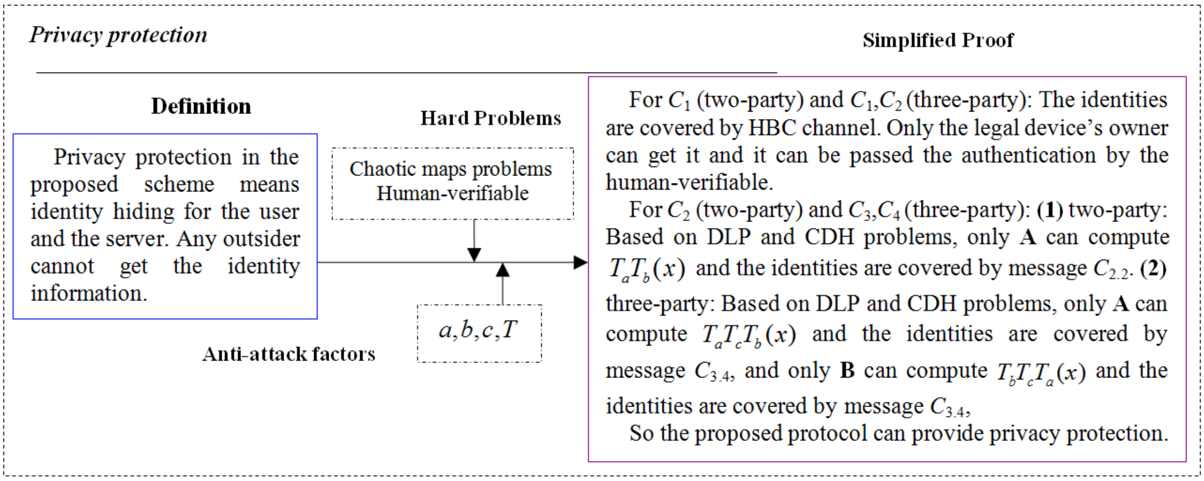


Protocols (Authentication phase)		[8] (2013)		Ours	
		Two-party	Three-party	Two-party	Three-party
Compu-tation	A	$4T_h + 1T_s + 2T_p$	$6T_h + 1T_s + 5T_p$	$3T_h + 2T_c$	$3T_h + 2T_c$
	B	$2T_h + 1T_s + 2T_p$	$7T_h + 1T_s + 5T_p$	$3T_h + 2T_c$	$4T_h + 2T_c$
	C		$8T_h + 1T_s + 6T_p$		$4T_h + 4T_c$
Comm-unication	Messages	6	13	5	11
	rounds	2	4	2	4
Design	Concise design	No	No	Yes	Yes
	Number of nonces	2	3	2	3
	Model	Random Oracle with human-verifiable		Random Oracle with human-verifiable	

4.2. **Other discussions.** This section uses flow charts to give the proof of some attacks simply. The Fig.5 Fig.10 describe the process of security proof privacy protection, Impersonation attack, Man-in-the-middle attack, Replay attack, Known-key security and Perfect forward secrecy respectively.

In the Table 4, some specific comparative results are shown between the proposed scheme and the related works.

5. **Efficiency Analysis.** Table 5 shows performance comparisons between our proposed scheme and the literatures of [8]. We sum up these formulas [22] into one so that it can reflect the relationship among the running time of algorithms intuitively. $T_p \approx 10T_m \approx 30T_c \approx 72.6T_s \approx 1263.24T_h$, where: T_p: Time for bilinear pair operation, T_m: Time for a point scalar multiplication operation, T_c: The time for executing the $T_n(x)$ mod p in



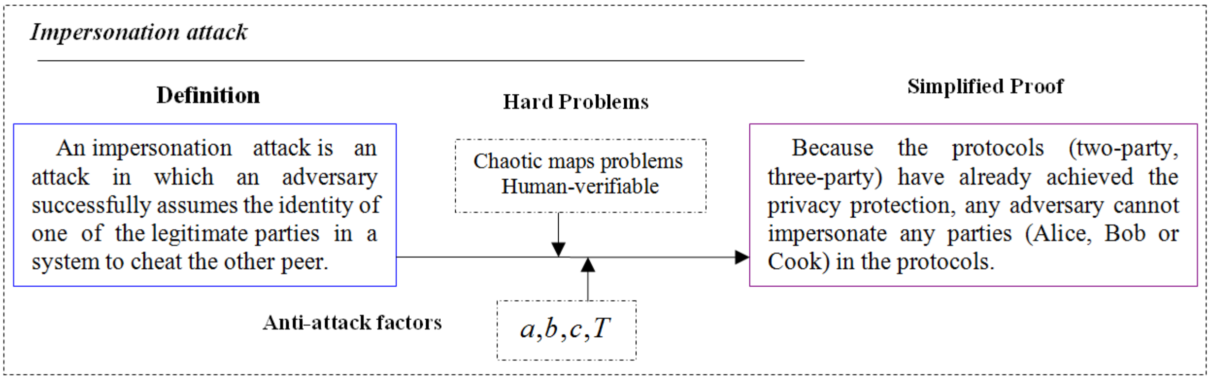
Privacy protection in the proposed scheme means identity hiding for the user and the server. Any outsider cannot get the identity information.

For C_1 (two-party) and C_1,C_2 (three-party): The identities are covered by HBC channel. Only the legal device's owner can get it and it can be passed the authentication by the human-verifiable.

For C_2 (two-party) and C_3,C_4 (three-party): **(1)** two-party: Based on DLP and CDH problems, only **A** can compute $T_aT_b(x)$ and the identities are covered by message $C_{2.2}$. **(2)** three-party: Based on DLP and CDH problems, only **A** can compute $T_aT_cT_b(x)$ and the identities are covered by message $C_{3.4}$, and only **B** can compute $T_bT_cT_a(x)$ and the identities are covered by message $C_{3.4}$,

So the proposed protocol can provide privacy protection.

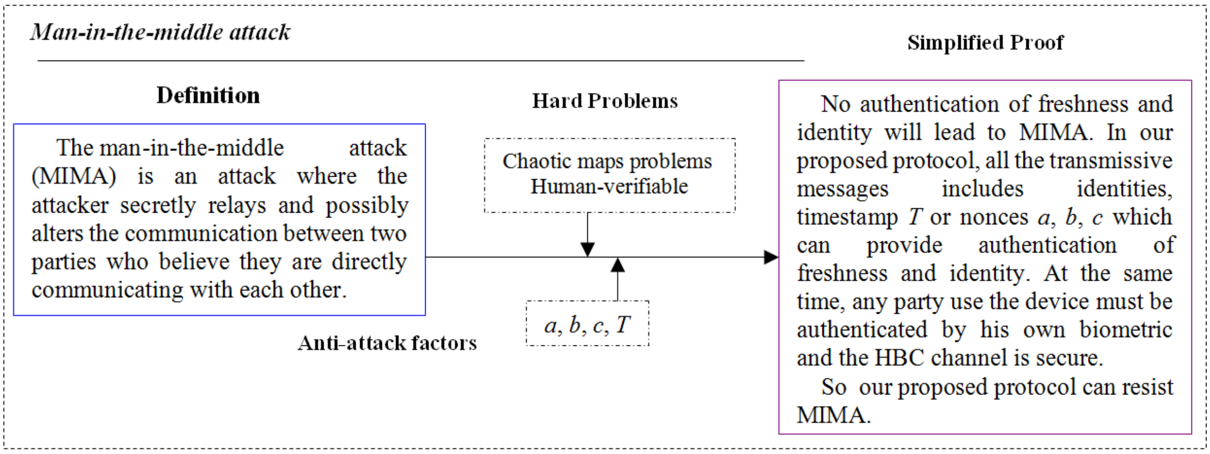
FIGURE 5. Proof about privacy protection for our proposed protocols



An impersonation attack is an attack in which an adversary successfully assumes the identity of one of the legitimate parties in a system to cheat the other peer.

Because the protocols (two-party, three-party) have already achieved the privacy protection, any adversary cannot impersonate any parties (Alice, Bob or Cook) in the protocols.

FIGURE 6. Proof about impersonation attack for our proposed protocols



The man-in-the-middle attack (MIMA) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

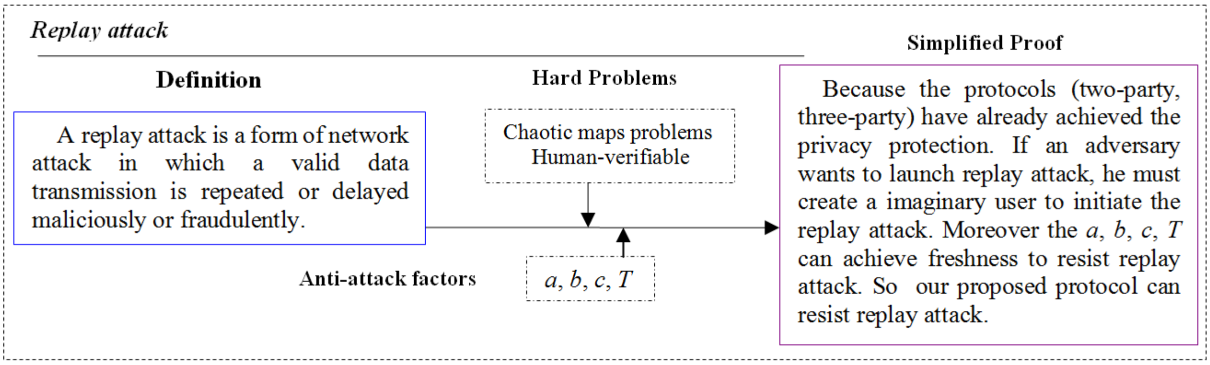
No authentication of freshness and identity will lead to MIMA. In our proposed protocol, all the transmissive messages includes identities, timestamp T or nonces a, b, c which can provide authentication of freshness and identity. At the same time, any party use the device must be authenticated by his own biometric and the HBC channel is secure.

So our proposed protocol can resist MIMA.

FIGURE 7. Proof about impersonation attack for our proposed protocols

Chebyshev polynomial, T_s: Time for symmetric encryption algorithm, T_h: Time for Hash operation.

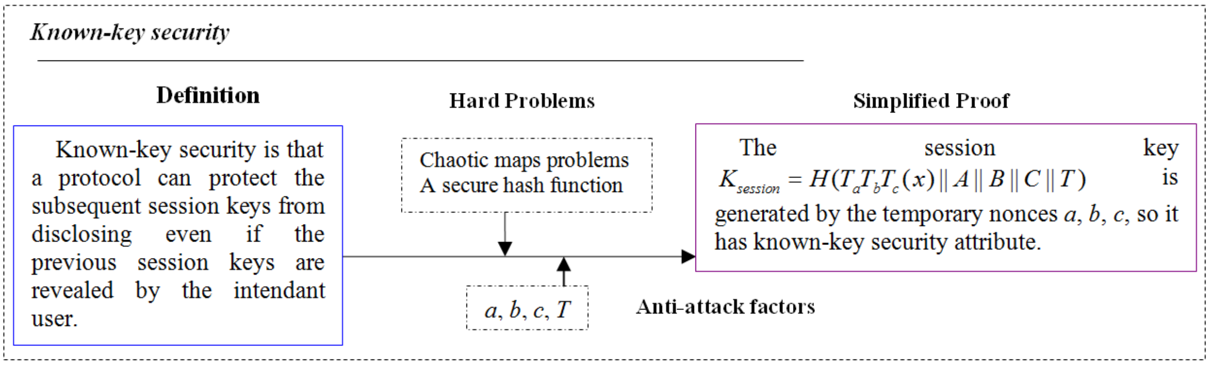
Based on Table 4 and Table 5, we can draw a conclusion that the proposed scheme has achieved an improvement in both efficiency and security.



A replay attack is a form of network attack in which a valid data transmission is repeated or delayed maliciously or fraudulently.

Because the protocols (two-party, three-party) have already achieved the privacy protection. If an adversary wants to launch replay attack, he must create a imaginary user to initiate the replay attack. Moreover the a, b, c, T can achieve freshness to resist replay attack. So our proposed protocol can resist replay attack.

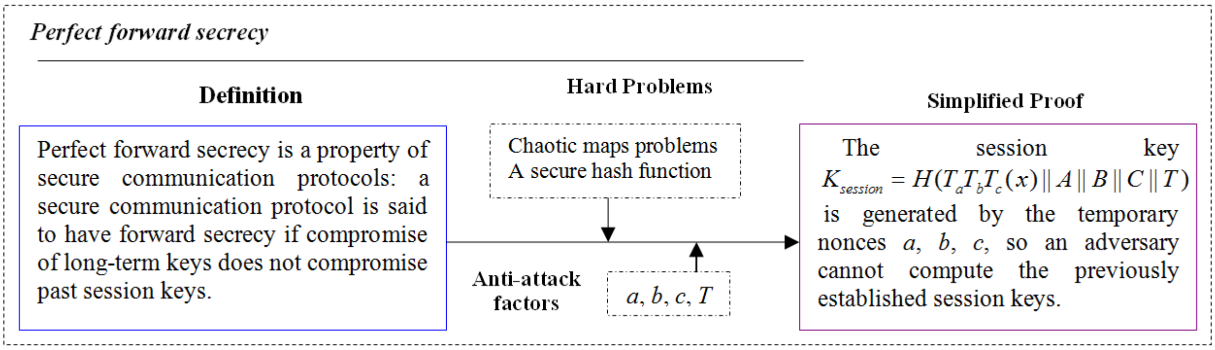
Figure 8. Proof about replay attack for our proposed protocols



Known-key security is that a protocol can protect the subsequent session keys from disclosing even if the previous session keys are revealed by the intendant user.

The session key $K_{session} = H(T_a T_b T_c(x) \| A \| B \| C \| T)$ is generated by the temporary nonces a, b, c, so it has known-key security attribute.

Figure 9. Proof about Known-key security



Perfect forward secrecy is a property of secure communication protocols: a secure communication protocol is said to have forward secrecy if compromise of long-term keys does not compromise past session keys.

The session key $K_{session} = H(T_a T_b T_c(x) \| A \| B \| C \| T)$ is generated by the temporary nonces a, b, c, so an adversary cannot compute the previously established session keys.

Figure 10. Proof about perfect forward secrecy for our proposed protocols

6. Conclusion.

In this paper, we design two kinds of human-verifiable privacy preserving protocols with HBC communication, which can effectively protect the privacy of mobiles users. To protect the users privacy, we used two kinds of hard problems: one is human-verifiable, which is used in the forward processes; the other is DLP and CDH problems, which are used in the backward processes. Finally, after comparing with related literatures respectively, we found our proposed scheme has satisfactory security, efficiency and functionality. Therefore, our protocol is more suitable for practical applications.

Acknowledgement. This work is supported by the Liaoning Provincial Natural Science Foundation of China (Grant No.201602680).

REFERENCES

[1] S. M. Bellovin and M. Merritt, Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and password file compromise, *in Proc. 1st ACM Conf. Comput. and Communications Security*, pp. 244-250, 1993.

[2] D. P. Jablon, Strong password-only authenticated key exchange, *ACM SIGCOMM Comput. Commun. Rev.*, vol. 26, no. 5, pp. 5-26, 1996.

[3] T.Wu, The secure remote password protocol, *in Proc. Symp. Internet Soc. Network and Distributed Syst. Security*, vol. 1, pp. 97-111, 1998.

[4] V. Boyko, P. MacKenzie, and S. Patel, Provably secure passwordauthenticated key exchange using Diffie-Heilman, *in Proc. Advances in Cryptology-Eurocrypt*, pp. 156-171 , 2000.

[5] M. Bellare and P. Rogaway, Entity authentication and key distribution, *in Proc. Advances in Cryptology-CRYPTO*, vol. 773, pp. 232-249, 1993.

[6] S. Blake-Wilson and A. Menezes, Entity authentication and authenticated key transport protocols employing asymmetric techniques, *in Proc. Security Protocols Workshop*, vol. 97, , 1997.

[7] J. M. McCune, A. Perrig, andM. K. Reiter, Seeing-is-believing: using camera phones for human-verifiable authentication,*in Proc. IEEE Symp. on Security and Privacy*, pp. 110-124, 2005.

[8] C. M. Chen, K. H. Wang, T. Y. Wu, J. S. Pan and H. M. Sun. A Scalable Transitive Human-Verifiable Authentication Protocol for Mobile Devices, *IEEE transaction son information forensics and security*, vol. 8, no. 8, August 2013

[9] R. Prasad, Human Bond Communication, *Wireless Pers Commun* , vol. 87, pp. 619-627, 2016.

[10] X. Guo, J. Zhang, Secure group key agreement protocol based on chaotic hash, *J. Inf. Sci.* vol. 180, no. 20, 4069-4074, 2010.

[11] H. F. Zhu, A Provable One-way Authentication Key Agreement Scheme with User Anonymity for Multi-server Environment, *KSII transaction son Internet and information systems*, vol. 9, no. 2, pp. 811-829, Feb. 2015.

[12] H. J. Wang, H. Zhang, J. Li and C. Xu. A(3,3) visual cryptography scheme for authentication, *Journal of Shenyang Normal University (Natural Science Edition* , vol.31, no.101, pp. 397-400, 2013.

[13] F. Ozkaynak, Cryptographically secure random number generator with chaotic additional input, *J. Nonlinear Dyn.*, vol. 78, no. 3, pp. 2015-2020, 2014.

[14] J. Chen, J. Zhou, K.W. Wong, A modified chaos-based joint compression and encryption scheme, *IEEE Trans. Circuits Syst. II Express Briefs,* vol. 58, no. 2, pp. 110-114, 2011.

[15] P. Bergamo, P. DArco, A.De Santis, L. Kocarev, Security of public-key cryptosystems based on Chebyshev polynomials, *IEEE Trans. Circuits Syst. I,* vol. 52, no. 7, pp. 1382-1393, 2005.

[16] S. J. Xu, , X. B. Chen, R. .Zhang , Y. X. Yang, Y. C. Guo, An improved chaotic cryptosystem based on circular bit shift and XOR operations, *J. Phys. Lett.* , vol. A 376, no. 10, pp. 1003-1010, 2012.

[17] K. Chain, W. C. Kuo, A new digital signature scheme based on chaotic maps, *J. Nonlinear Dyn* , vol. 74, pp. 1003-1012, 2013.

[18] H. F. Zhu, Flexible and Password-Authenticated Key Agreement Scheme Based on Chaotic Maps for Multiple Servers to Server Architecture, *Wireless Pers Commun.*, vol. 82, no. 3, pp. 1697-1718, 2015.

[19] T. H, Jan R, Yang W, A chaotic maps-based key agreement protocol that preserves user anonymity, *In: IEEE International Conference on Communications (ICC09)*, pp. 1-6, 2009.

[20] M. Burrows, M., Abadi, R. Needham, A logic of authentication. ACM Trans, *J. Comput. Syst.,* vol. 8, pp. 18-36 , 1990.

[21] L. Kocarev, and S. Lian, Chaos-Based Cryptography: *Theory, Algorithms and Applications*, pp. 53-54, 2011.

[22] T. Y. Wu and Y. M. Tseng, An ID-based mutual authentication and key exchange protocol for low-power mobile devices, *The Computer Journal*, vol. 53 , no.7, pp. 1062-1070, 2010.

[23] T. Y. Wu and Y. M. Tseng, An efficient user authentication and key exchange protocol for mobile client-server environments, *J. Computer Networks*, vol. 54 , no. 9, pp. 1520-1530, 2010.