Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2015, Article ID 764919, 11 pages
http://dx.doi.org/10.1155/2015/764919

*Research Article*

# Securing Body Sensor Networks with Biometric Methods: A New Key Negotiation Method and a Key Sampling Method for Linear Interpolation Encryption

**Huawei Zhao,[1] Chi Chen,[2] Jiankun Hu,[3] and Jing Qin[4]**

[1]*Department of Internet Finance, Qilu University of Technology, Jinan 250100, China*
[2]*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China*
[3]*School of Engineering and Information Technology, University of NSW (UNSW) at the Australian Defence Force Academy (ADFA), Canberra, ACT 2600, Australia*
[4]*School of Mathematics, Shandong University, Jinan 250100, China*

Correspondence should be addressed to Jiankun Hu; j.hu@adfa.edu.au

Received 7 June 2014; Accepted 22 October 2014

Academic Editor: Rongbo Zhu



We present two approaches that exploit biometric data to address security problems in the body sensor networks: a new key negotiation scheme based on the fuzzy extractor technology and an improved linear interpolation encryption method. The first approach designs two attack games to give the formal definition of fuzzy negotiation that forms a new key negotiation scheme based on fuzzy extractor technology. According to the definition, we further define a concrete structure of fuzzy negotiation that can enlarge the types of biometric data used to negotiate shared keys between biosensor nodes. The second approach includes a detailed key sampling method that uses shared secrets to generate linear interpolation factors and an improved linear interpolation encryption scheme based on linear equation group. Security analyses show that these two approaches are secure and can resist attacks launched by Ultra-Wide Band (UWB) technology, which has not received due attention in the existing studies.

## 1. Introduction

Body sensor networks (BSNs) are an important branch of wireless sensor networks (WSNs) [1, 2]. A BSN is a medical information system in the field of e-health, and it consists of some biosensor nodes that form a wireless micronetwork on the human body. These biosensor nodes are microscale equipment integrated with biosensors and transceivers [3], and they can provide a capability of automated and continuous human monitoring when they are worn on or implanted in the human body. At present, various biosensors have been designed to measure diverse physiological signals, such as blood pressure (systolic and diastolic), electrocardiogram (ECG), blood oxygen level (SpO2), and activity recognition. These sensors are available in many different forms, including wrist wearable devices, implantable devices, and biomedical smart clothes [4–7]. Based on the functions of biosensors, BSNs cannot only monitor body health, but also perform complete intelligent treatment, such as accurate insulin injection. Applications of BSNs will greatly improve the society's medical conditions and promote living qualities of people.

In order to realize exchanging of medical information among biosensor nodes in a BSN, physiological signals should be transformed into biometric data. Since these data are sensitive medical information, they must be protected. Otherwise, the leaked biometric data could divulge personal privacy, and the tampered biometric data could cause serious medical accident and even threaten a patient's life [8–11]. National regulations are being established to ensure the privacy and security of healthcare data from data generation, transmission, storage, and usage. For example, the HIPAA (the Health Insurance Portability and Accountability Act) has set a benchmark [8]. However, the computational and bandwidth limitations of BSNs are on a par with those

found in the so-called microsensor networks, which make traditional security paradigms [12–17] designed for conventional WSNs not directly applicable to BSNs. Thus, there are great challenges in designing security schemes for BSNs. One of the core problems is how to establish shared keys among biosensor nodes and how to encrypt biometric data efficiently. Note that biometric data themselves have an advantage over conventional cryptography in authenticating genuine users [18, 19]; a natural solution of protecting biometric data will be the combination of conventional cryptography and biometric security method, for example, as discussed in biocryptography [20, 21].

Due to physiological noise and errors of biosensors, the same kind of biometric data collected by various biosensors may not have the exact same value, which causes these data to be not suitable to be used in key negotiation directly. To solve the problem, a common method is to use error-correcting codes [17, 22]. In addition, linear interpolation encryption method has great advantages over conventional encryption methods in protecting biometric data [23]. However, both of the methods have drawbacks, respectively. In the former method, common keys only can be derived from error-correcting codes, which stringently limits the size of key space. In addition, the method only can use high-entropy physiological signals to negotiate common keys, but at present people only recognize a few kinds of high-entropy physiological signals in the human body, which means that the method has not a good application prospect. Also the latter method does not provide idea on how to sample interpolation factors from the physiological signals, and it cannot resist the attack of remotely collecting physiological signals launched by the Ultra-Wide Band (UWB) technology. In order to address the above problems, we introduce predeployed keys technology and fuzzy extractor to build key negotiation scheme and propose a new biometric data encryption scheme. Our contributions include the following: (i) we design a fuzzy-extractor-based key negotiation scheme using error-correcting codes and predistributed keys, and the scheme has stronger security and is easier to use in practice; (ii) to remedy the drawbacks in the linear interpolation encryption shown in [23], we give a concrete method of sampling interpolation factors from physiological signals and propose a more secure encryption method for biometric data.

The rest of the paper is organized as follows. Section 2 presents the existing research results related to key negotiation and biometric data encryption in BSNs and analyzes the known security problems. Section 3 proposes a new key negotiation scheme based on fuzzy extractor technology and analyzes security of the new scheme. A detailed method of sampling linear interpolation factors and an improved linear interpolation encryption scheme are developed and their security analyses are given in Section 4. Finally, in Section 5 conclusions are drawn.

## 2. Related Work

*2.1. Fuzzy Commitment Technology.* In a human body, some biometric data have a high level randomness and can be viewed as pseudorandom numbers, and thus, these data can be used to build key negotiation schemes in BSNs. Reference [24] proposed using a group of similar random numbers generated from these biometric data at different sites of the human body to encrypt and decrypt a symmetric key for secured distribution. Since the same biometric data captured at different locations of the body have slight differences, they employed a fuzzy commitment technology [22] to ensure that errors in a recovered encryption key can be removed by a certain error-correcting code $C$. At the transmission terminal, a high-entropy biometric value $x$ is used by a biosensor node A to commit the key $k_{\text{shared}}$ that is an element of $C$, say, using $F(k_{\text{shared}}, x) = h(k_{\text{shared}}) \| (x \oplus k_{\text{shared}})$, where $h(\cdot)$ is a hash function, $\oplus$ is the bitwise XOR operation, and $\|$ means concatenation. At the receiving terminal, if the same kind of biometric value $x'$ collected by the other biosensor node B is similar to $x$, and the difference between them is tolerable to $C$, B can use $x'$ and $C$ to decommit the key $k_{\text{shared}}$. Compared with traditional key negotiation schemes, the noninteractive fuzzy commitment scheme has less energy consumption in messages transmission and is suitable for BSNs. Next, various algorithms have been developed following the work of [24]. In [23], a method was proposed, which only transfers commitments to complete keys negotiation. The method is conductive in reducing messages transferred for negotiation of shared keys and is suitable to negotiate shared keys among more than two biosensor nodes. Reference [25] used a hybrid topology that combines two topologies, star and mesh, to establish shared keys. In the scheme, identities of biosensor nodes are used to authenticate shared keys, and a mechanism of changing cluster heads according to energy is proposed to maximize the lifetime of BSNs. Reference [26] proposed a method that uses time slots to solve synchronization problem of high-entropy biometric data between biosensors. Reference [27] pointed out by experiment that the timing information of heartbeats has high-entropy characteristic and can be used to negotiate shared keys in BSNs. Reference [28] proposed an energy efficient key management for BSNs based on fuzzy commitment where a weak time synchronization mechanism and an energy-based multi-hop-route-choice method are advanced to decrease the energy of key management in BSNs.

Although many achievements have been made on this topic, several challenging security problems remain. (1) Only variable and high-entropy biometric data in the human body are considered for negotiating keys. Up to now, only the timing information of heartbeats has been proved to satisfy the requirement [27], which greatly limits applications of the technology in practice. (2) Shared keys are only generated from the set of error-correcting codes, which restrict the choice space of keys. Furthermore, some researchers argue that the generation may cause security problems for the reason that error-correcting codes should be public, and adversaries could easily get $k_{\text{shared}}$ by its hash value [29]. (3) Shared keys are vulnerable to a new developing RCB (remotely capturing biometric data) attack that uses UWB (Ultra-Wide Band Radar) technology to remotely capture some kinds of biometric data [27]. That is, when an adversary remotely captures a biometric value $x$ that is used to negotiate shared keys and eavesdrops the corresponding commitment:

$p = x \oplus k_{\text{shared}}$, he can easily get the shared key by: $p \oplus x = x \oplus k_{\text{shared}} \oplus x = k_{\text{shared}}$.

*2.2. Fuzzy Extractor Technology.* Following the development of the fuzzy commitment technology, another biometric cryptography, fuzzy extractor technology, was proposed in [30]. A fuzzy extractor is composed of two procedures (Gen, Rep) that operate as follows. Suppose $W$ is a variable and $w$ and $w'$ are two values of $W$. The first procedure (Gen) in the transmission terminal holds $w$, if it wants to establish a shared secret $R$ with the second procedure (Rep) in the receiving terminal, it computes $(R, P) = \text{Gen}(w)$ and sends $P$ to Rep; Rep holds $w'$, and when it receives $P$, it computes $R' = \text{Rep}(w', P)$. A fuzzy extractor satisfies correctness if $R = R'$ when the distance between $w'$ and $w$ is tolerable to a selected error-correcting code and satisfies security if $R$ is uniformly distributed even given $P$ when the entropy of $W$ is high. The main difference between fuzzy commitment and fuzzy extractor lies in the fact that the former's goal is to recover the original key of transmission terminal at the receiving terminal, and the latter's goal is realize the reproduction of a secret $R$ from $w'$ close to $w$ at the receiving terminal after the transmission terminal generates $R$ from $w$.

When $w$ is looked at as a biometric template, fuzzy extractor can be used widely in the fields of secure authentication and key reproduction, which cause it to be well studied. Reference [31] pointed out that an improper sketch construction and a biased error-correcting code are both the source of leaking secret biometric data; they make a fuzzy extractor not adequate for multiple use of the same secret biometric data. And then, it proposed two concepts, "outsider chosen perturbation security" and "insider chosen perturbation security," to address the security problem. Reference [32] pointed out that fuzzy extractor cannot resist active attack, and when commitments are tampered, the authentication service provided by fuzzy extractor will be invalid. And then, it used ideal hash function to build a robust extractor to resist this kind of active attack. Reference [33] showed that some of more popular constructions that have been shown before have serious security weaknesses in presence of even very weak adversaries. And then, it proposed two concepts, indistinguishability and irreversibility, and designed two attack games to define the security of fuzzy extractor. Reference [34] explained the root of vulnerability of fuzzy extractor; that is, because the key derived from biometric data must be indistinguishable to uniform random distribution, the leakage of information associated with the biometric data is unavoidable. And following the work of [33], it further divided the concept of indistinguishability into two security levels, "weak biometric privacy" and "strong biometric privacy," and according to the two security levels, it advanced a method to improve the security of fuzzy extractor. Following the above researches [35], proposed a robust fuzzy extractor structure and an authenticated key agreement from close biometric data. The research considered both keyless case and keyed case of building shared keys and gave solutions to reduce the loss of entropies in the negotiation of shared keys.

Fuzzy extractor has advantages over fuzzy commitment in terms of key space and option of biometric data, while it cannot be used directly to negotiate shared keys in BSNs scenario. That is, due to real-time physiological noise and errors of biosensors, the distance between the template of biometric data and the same kind of biometric data collected in real time by other biosensors always is out of toleration of the selected error-collecting code. In addition, the existing key management schemes based on fuzzy extractor technology are always not suitable to practical BSNs; for instance, key agreement scheme in [35] cannot resist the new developing RCB attack, and furthermore it only uses biometric data with high entropy to negotiate shared keys.

*2.3. INTRAS Encryption.* In order to improve the efficiency of encrypting biometric data in BSNs, [23] proposed a set of linear interpolation encryption schemes, called INTRAS, which are effectively a combination of interpolation and random sampling. The simplest scheme of INTRAS is summarized as follows.

(1) In a BSN context, the shared encryption key $k$ is used to generate a vector of sampling instants $d = \langle d[1], d[2], \ldots, d[n] \rangle$ by both the sender and the receiver.

(2) For the sender, on input sequence $x = \langle x[1], x[2], \ldots, x[n] \rangle$, an interpolation filter outputs a sequence of concrete interpolated signals $x_c = \langle x_c[1], x_c[2], \ldots, x_c[n] \rangle$.

(3) At each instant $i$, the resampling block simply resamples the interpolated signal $x[i]$ using a delay $d[i]$ to produce the scramble output $x_c[i]$ by

$$x_c[i] = d[i] \cdot x[i] + (1 - d[i]) \cdot x[i-1], \quad (1)$$

where $1 \le i \le n$ and $x[0]$ is an initial value.

Here, security is achieved from the fact that the input cannot be recovered from the scrambled output $x_c[i]$, without knowledge of the delay vector $d$.

(4) For the receiver, on input sequence $x_c$ and $d$, he can recover the sequence $x$.

The simplest INTRAS encryption has two problems. One is that [23] does not give the concrete method to generate interpolation factors, and the problem exists in all of the other forms of INTRAS encryption schemes; the other one is that knowing the input data and encrypted output is equivalent to knowing the key, which is vulnerable to the RCB attack. Though other forms of INTRAS encryption do not have the latter problem, their procedures are too complicated to realize.

From the above analyses, it can be seen that existing researches cannot secure BSNs effectively, so in the rest of the paper, we first combine the technologies of predeployed keys and fuzzy extractor to design a new key negotiation method, called fuzzy negotiation. And then, we propose a detailed method to generate interpolation factors sequence from shared secrets and further advance an improved INTRAS encryption method.

## 3. Proposed Fuzzy Negotiation Technology for Key Negotiation

In this section, we make use of predeployed keys technology and fuzzy extractor technology to propose a new key negotiation method. Our goal is threefold, (i) to enlarge the key space by combing predeployed keys and physiological signals; (ii) to use physiological signals with any entropies to negotiate common keys; (iii) to resist the RCB attack.

*3.1. Definition of Fuzzy Negotiation.* Like fuzzy commitment and fuzzy extractor, fuzzy negotiation makes use of error-correcting codes to negotiate keys. Let $M$ be a space of messages with distance function dist$(\cdot)$; more formally an error-correcting code $C$ is a subset of $K$ number of distinct codewords $\{c_0, \ldots, c_{k-1}\}$ of $M$. The Hamming distance of $C$ is the smallest $d$ such that $\text{dist}(c_i, c_j) \geq d$ for all $i \neq j$, which means that $C$ can detect up to $d - 1$ errors, and the error-correcting distance is $t = \lfloor (d-1)/2 \rfloor$ [17].

As our work is in the computational setting, we use $\kappa$ to denote the security parameter. All algorithms are assumed to be a polynomial time in $\kappa$. Then a function $\varepsilon(\kappa)$ is negligible if for all positive polynomial $p(\cdot)$ and sufficiently large $\kappa, \varepsilon(\kappa) \leq 1/p(\kappa)$.

In a BSNs, let $K$ denote the preloaded secret of all biosensor nodes, $W$ is a variable of $M$ with length $|W| = l$, $w$ and $w'$ are values of $W$, $r$ is a random value with length $l$, and $t$ is the error-correcting distance of a selected public error-collecting code $C$, where the length of each codeword $c$ is $l$. Then, we give a formal definition of fuzzy negotiation as follows.

*Definition 1.* A structure of fuzzy negotiation is a pair of randomized procedures, "Trans" and "Rec," with the following properties.

(1) On input $w$, $K$, $r$, and $c$, the generation procedure "Trans" outputs an extracted secure string $R \in \{0,1\}^l$ and a public string $P \in \{0,1\}^*$ to commit $R$.

(2) *Correction*. The reproduction production "Rec" takes an element $w'$ and a public string $P \in \{0,1\}^*$ as inputs. The correctness property of fuzzy negotiation guarantees that if $\text{dist}(w, w') \leq t$, and $R$, $P$ are generated by $(R, P) \leftarrow \text{Trans}(K, w, r, c)$, then $\text{Rec}(K, w', P, C) = R$. If $\text{dist}(w, w') > t$, then no guarantee is provided about the output of "Rec."

(3) *Security*. Any adversary wins the adaptively chosen biometric data attack game and adaptively chosen commitment attack game defined as follows with negligible possibilities.

*Adaptively Chosen Biometric Data Attack Game*. We define an adaptively chosen biometric data attack game against fuzzy negotiation as the following game between a challenger and an adversary. In the initialization, the challenger is assigned with a secret $K$.

*Preparation.* The adversary chooses a kind of physiological signal and describes it as a biometric variable $W \in M$. Then, the adversary gives the specification of $W$ (such as the kind of the physiological signal) to the challenger.

*Queries.* The adversary makes up to $q$ possibly adaptive queries. To form adaptive query $i$, the adversary produces a value $w_i$ of $W$, a random value $r$, and a codeword $c$ from $C$ and then sends all of them to the challenger. The challenger produces $(P_i, R_i) \leftarrow \text{Trans}(K, w_i, r, c)$ and sends $P_i$ to the adversary.

*Challenge.* The adversary produces a value $w$ of $W$, a random value $w'$ with length $|w|$, and a random value $r$ and selects a codeword $c$ from $C$ and then sends all of them to the challenger. The challenger randomly produces a bit $b$; if $b = 1$, the challenger computes $(P^*, R^*) \leftarrow \text{Trans}(K, w, r, c)$, and if $b = 0$, the challenger computes $(P^*, R^*) \leftarrow \text{Trans}(K, w', r, c)$ instead. Finally, the challenger sends $P^*$ to the adversary.

*More Queries.* The adversary runs additional queries as described in step "Queries."

*Response.* The adversary eventually produces a bit $b'$ and wins if $b' = b$.

Let adversary$(P^*)$ be the output of the adversary when it gets $P^*$ and $w \mid w'$ an alternative choice with a probability of 1/2. Then, the adversary's advantage in this game is defined as $\text{adv}^{Acb}(\kappa) = |\Pr[b \leftarrow \text{adversary}(P^*) P^* = \text{Trans}(K, ww', r, c)] - 1/2|$.

**Theorem 2.** *The fuzzy negotiation can withstand an adaptively chosen biometric data attack, if for any PPT (probability polynomial time) adversary, it holds that* $adv^{Acb}(\kappa) \leq \varepsilon(\kappa)$ *for a negligible small* $\varepsilon(\kappa)$.

*Proof.* The attack game simulates adaptive attack to the "Trans" procedure of fuzzy negotiation in practice: an adversary can adaptively capture some kind of biometric value $w$ (such as timing information of heartbeats) by RCB (remote capturing biometric data) attack and get the corresponding commitment $P$ by eavesdropping method. In such way, the adversary can do enough adaptive exercises to analyze the relationships between biometric data and corresponding commitments. If in such attacks, the adversary's advantage is negligible in step "Challenge," it means that the adversary cannot find the relationships between them, and then, the attacker cannot make use of commitments to compute biometric data, which cannot be captured remotely. □

*Adaptively Chosen Commitments Attack Game*. Let $\Delta$ be the set of perturbation functions over a messages space $M$; that is, $\Delta = \{\delta : M \rightarrow M\}$, where $\text{dist}(w, \delta(w))$ can be greater than $t$. We define an adaptively chosen commitments attack game against a fuzzy negotiation as the following game between a challenger and an adversary. In the initialization, the challenger is assigned with an error-correcting code $C$ and a secret $K$.

*Preparation.* The adversary points a kind of physiological signal as a biometric variable $W \in M$. And then, the adversary

gives the specification of $W$ (such as the kind of the physiological signal) to the challenger.

*Public Queries*. The adversary makes up to $q$ possibly adaptive queries: to form adaptive query $i$, the adversary produces a value $w_i$ of $W$, a random value $r$, and chooses a codeword $c$ from $C$ and then sends all of them to the challenger. The challenger produces $(P_i, R_i) \leftarrow \mathrm{Trans}(K, w_i, r, c)$ and sends $P_i$ to the adversary.

*Keys Queries*. The adversary makes up to $q'$ possible adaptive reproduction queries that can be interspersed with public queries as follows. To form query $i$, the adversary chooses $\delta_i' \in \Delta$, a biometric value $w'$, and $P'$ that is generated from $w'$ in the "public queries" step and then sends them to the challenger. The challenger computes $R_i' = \mathrm{Rec}(K, \delta_i'(w'), P_i', C)$ and returns $R_i'$ to the adversary. In order to let the adversary do enough exercises, the procedure "Rec" will return the adversary a value, such as a fault $R_i'$; even $\delta_i'$ satisfies $\mathrm{dist}(w', \delta_i'(w')) > t$.

*Challenge*. The adversary chooses $P^* \in \{P_1, \ldots, P_q\}$ from strings returned by the challenger in a public query and in any key query $(\delta_i', w', P^*)$ the distance has $\mathrm{dist}(w', \delta_i'(w')) > t$. The adversary sends $P^*$ to the challenger. The challenger randomly produces a bit $b$; if $b = 1$, the challenger computes $R' = \mathrm{Rec}(K, w', P^*, C)$ with unperturbed $w'$ and gives it to the adversary. Otherwise, if $b = 0$, it chooses a random string with length of $|R'|$ and gives it to the adversary instead.

*More Queries*. The adversary runs additional queries as described in step "Public Queries."

*Response*. The adversary eventually produces a bit $b'$ and wins if $b' = b$.

The adversary's advantage in this game is defined as $\mathrm{adv}^{Acc}(\kappa) = |\Pr[b \leftarrow \mathrm{adversary}(key) R = \mathrm{Rec}(K, w', P^*, C)] - 1/2|$.

**Theorem 3.** *The fuzzy negotiation can withstand the adaptively chosen commitments attack in $\Delta$, if, for any PPT adversary, it holds that $adv^{Acc}(\kappa) \leq \varepsilon(\kappa)$ for a negligible small $\varepsilon(\kappa)$.*

*Proof.* The attack simulates the adaptively chosen commitments attack to the "Rec" procedure of fuzzy negotiation in practice. Before a user uses a BSN product, an adversary can get the BSN product by some means (e.g., the adversary unpacks the BSN product unauthorizedly in the transportation) to launch adaptively chosen commitments attack where, for a pair of biometric value and commitment adaptively chosen, the adversary can get corresponding shared key. So, the adversary can do enough adaptive exercises to analyze the relationships between commitments and corresponding shared keys. □

*3.2. The Characteristics of Definition of Fuzzy Negotiation.* The definition of fuzzy negotiation is similar to that of fuzzy extractor, and the main difference lies in that the security in fuzzy negotiation is in the computational setting and is defined by two attack games. The reason is that fuzzy negotiation is used in key negotiation of BSNs, and the two attack games can emulate real attacks well on BSNs where the new RCB attack is included. In addition, we explicitly point out that error-correcting code $C$ is public, and its codewords can be known by the adversary, which meets the common usages of error-correcting code and is in accordance with the opinion in [29].

Our adaptively chosen biometric data attack game looks similar to the "weak biometric privacy" game introduced in [33]. However, their applications are different in essence. The "weak biometric privacy" game is used to describe the attack to biometric data based authentication that uses fuzzy extractor technology. In order to launch such an attack, the adversary needs to obtain the same kind of biometric trait that is already used as an authentication template. Due to differences in sampling biometric data each time from the human body, the game introduces a set of perturbation functions to simulate the differences, whereas our adaptively chosen biometric data attack game is used to describe the adversary's ability to analyze the relationships between biometric data and their commitments. When designing the game, it is observed that the RCB attack can contain some kinds of biometric data from the human body, which can pose serious threat to the security of BSNs. Our game does not need perturbation functions because the adversary is allowed to know the biometric data that are used to produce commitments. In step "Challenge," the adversary in former game does not know the perturbation function selected by the challenger and the biometric data which he wants to challenge. These restrictive conditions will decrease adversary's attacking ability. Whereas the adversary in our game knows the biometric data, the random value $r$ and the codeword $c$, all of them, are used to generate the challenge in step "Challenge." Furthermore, our adaptively chosen biometric data attack game implies that the adversary could analyze the relationship between biometric data and their commitments in "Queries," "Challenge," and "More Queries" steps. Thus, our adaptively chosen biometric data attack game is not only suitable for describing the attacks to BSNs, but also a stronger attack model.

In addition, our adaptively chosen commitments attack game is similar to the "strong biometric privacy" game specified in [33]. However, unlike the "strong biometric privacy" game, our adaptively chosen commitments attack game does not do any "key queries" in step "More Queries," which follows the fact that when BSN product is deployed on the user's body, the BSN is under surveillance all the time. The adversary has no chance to do "key queries" exercises. Furthermore, our adaptively chosen commitments attack game implies that the adversary could use $c$ to analyze the relationship between biometric data and their commitments and between commitments and corresponding shared keys in "Public Queries," "Private Queries," "Challenge," and "More Queries" steps.

*3.3. Structure of Fuzzy Negotiation.* According to the definition in Section 3.1 we design a fuzzy negotiation structure as follows. The structure consists of a pair of procedures: "Trans"

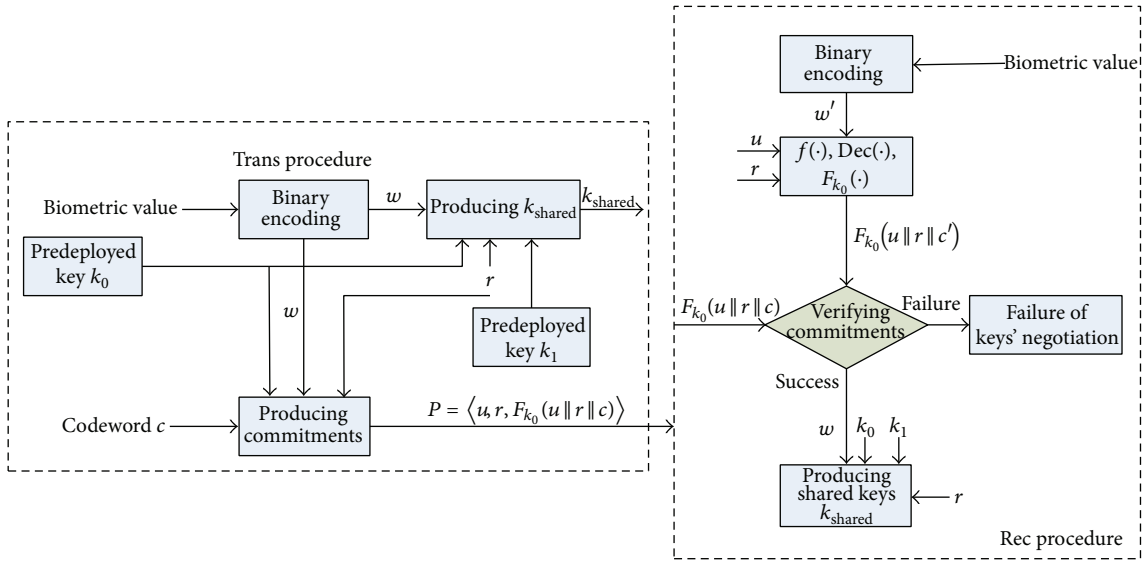


Figure 1: Structure of fuzzy negotiation.

and "Rec." As mentioned in Section 3.1, in the initialization of the structure, each biosensor node is preloaded with a secret $K$ that is divided into two keys, $k_0$ and $k_1$, with $|k_0| = |k_1| = l$. In addition, each biosensor node is assigned with a keyed one-way pseudorandom function $F_k(\cdot) : \{0,1\}^l \rightarrow \{0,1\}^l$ with $|k| = l$, an error-correcting function Dec(·) belonging to a selected error-correcting code $C$ and a function $f(\cdot) : \{0,1\}^l \times \{0,1\}^l \rightarrow \{0,1\}^l$ that satisfies $z = f(x,y) \Rightarrow y = f(x,z) \Rightarrow x = f(z,y)$.

(1) Procedure "Trans":

(i) collecting a biometric value from a pointed physiological signal and encoding it into a binary value $w$ with $|w| = l$;

(ii) selecting a codeword $c$ from the error-correcting code $C$ and computing the relationship between $c$ and $w : v = f(w,c)$;

(iii) generating an open random value $r$ with $|r| = l$ and then using $F(\cdot)$ to hide $v : u = v \oplus F_{k_0}(r)$;

(iv) finally, deriving the shared key: $k_{\text{shared}} = F_{k_0}(F_{k_1}(w \oplus r))$ ($\oplus$ is bitwise XOR operation) and outputting the commitment corresponding $w : P = \langle u, r, F_{k_0}(u \| r \| c) \rangle$ ("$\|$" denotes connection of messages).

(2) Procedure "Rec":

(i) collecting the same kind of biometric value and encoding it into a binary value $w'$ with $|w'| = l$;

(ii) using the predeployed key $k_0$ to recover the relationship $v : v = u \oplus F_{k_0}(r)$;

(iii) encoding $w'$ and $v$ into $c^* : c^* = f(w', v)$ which is a fuzzy version of $c$;

(iv) using Dec(·) to correct $c^* : c' = \text{Dec}(c^*)$. If $F_{k_0}(u \| r \| c) = F_{k_0}(u \| r \| c')$, the correction is successful, and $w$ can be recovered as $w = f(v,c)$. And then, the shared key can be reproduced as $k_{\text{shared}} = F_{k_0}(F_{k_1}(w \oplus r))$. Otherwise, if $F_{k_0}(u \| r \| c) \neq F_{k_0}(u \| r \| c')$, it means the failure of shared keys' negotiation.

The structure of fuzzy negotiation is shown in Figure 1.

In hospital applications, many BSNs on various patients' bodies may overlap in their wireless range. If biometric data collected by two biosensor nodes that have been placed on two adjacent patients' bodies, respectively, are similar, the two biosensor nodes belonging to two different subjects can negotiate a shared key, which will cause serious medical accidents. However, many existing schemes [22–27] have ignored this problem. In our scheme, the preloaded $k_0$ and $k_1$ in a BSN are different from the ones in other BSNs, which ensures that a biosensor node can only negotiate shared keys with the biosensor nodes in the same BSN.

*3.4. Correction Analysis of Fuzzy Negotiation.* For simplicity, we define $f(\cdot)$ as bitwise XOR operation $\oplus$, and then in procedure "Trans" $v$ and $u$ can be defined as $v = w \oplus c$ and $u = w \oplus c \oplus F_{k_0}(r)$, respectively. Accordingly, $P$ can be defined as $\langle w \oplus c \oplus F_{k_0}(r), r, F_{k_0}(w \oplus c \oplus F_{k_0}(r) \| r \| c) \rangle$, and the shared key can be defined as $k_{\text{shared}} = F_{k_0}(F_{k_1}(w \oplus r))$.

In procedure "Rec," $c^*$ can be defined as $c^* = f(v, w') = u \oplus F_{k_0}(r) \oplus w' = w \oplus c \oplus w' = e \oplus c$, where $e$ is the difference between $w$ and $w'$. If $e \leq t$, procedure "Rec" can recover $c$ by the error-correcting function Dec(·) which causes $F_{k_0}(u \| r \| c) = F_{k_0}(u \| r \| c')$. And then, procedure "Rec" can recover $w$ by $w = f(v,c)$ to generate $k_{\text{shared}} = F_{k_0}(F_{k_1}(w \oplus r))$ which is shared with procedure "Trans." If $e > t$, procedure "Rec" cannot recover $c$ effectively, and the key negotiation fails.

*3.5. Security Analysis of Fuzzy Negotiation.* Here we also define $f(\cdot)$ as bitwise XOR operation $\oplus$. Let $l = 128$ bits, $f(\cdot) : \{0,1\}^{128} \times \{0,1\}^{128} \to \{0,1\}^{128}$, and $F_{k_0}(\cdot) : \{0,1\}^{128} \to \{0,1\}^{128}$. In the following, we analyze security of fuzzy negotiation according to the two attack games: adaptively chosen biometric data attack game and adaptively chosen commitments attack game. Firstly, we suppose that a 128-bit value is secure to the exhaustive attack, the adversary can get biometric value $w$ by RCB attack, and the error-correcting code $C$ is open.

In the former attack game, when the adversary gets commitment $P = \langle w \oplus c \oplus F_{k_0}(r), r, F_{k_0}(w \oplus c \oplus F_{k_0}(r) \| r \| c) \rangle$, it can compute $F_{k_0}(r)$. Since $F_{k_0}(\cdot)$ is a keyed one-way function, the adversary can only guess the right $k_0$ from $F_{k_0}(r)$ and $r$ with a negligible probability. Then, we can say that although the adversary can get a biometric value by RCB attack and its commitment by eavesdropping, it hardly finds the relationship between them with a negligible probability. In other words, the adversary can win the former attack game with a negligible probability. In the situation, the adversary cannot launch RCB attack to a biometric value which he cannot capture remotely as he cannot deduce the biometric value by its public commitment. This can protect these biometric data from being known by the adversary.

In the latter attack game, the adversary can obtain enough pairs of $w$ and $\mathrm{Rec}(K, \delta(w), P, C) = F_{k_0}(F_{k_1}(w \oplus r))$. Although $w$, $r$, and $F_{k_0}(F_{k_1}(w \oplus r))$ are known to the adversary, it will search the key space of $2^{128} \times 2^{128}$ before obtaining the right $k_0$ and $k_1$, which is an infeasible task. Then, without $k_0$ and $k_1$, the adversary can hardly compute the relationship between the commitment of $w$ and the shared key $k_{\text{shared}}$, even given $w$, $\delta(w)$, and $C$. Thus, we can say that the adversary wins the latter attack game with a negligible probability.

It is worth noting that, in fuzzy negotiation, we do not require that $w$ must be a high-entropy biometric value. The reason is that, in the equation $k_{\text{shared}} = F_{k_0}(F_{k1}(w \oplus r))$, $r$ is a random value and $F_k(\cdot)$ is a keyed pseudorandom function, which causes the input of $F_{k_0}(\cdot)$ to be a secret value that is computing-indistinguishable from a uniformly random value even $w$ is a constant value. Thus, in the "Key Queries" step of the adaptively chosen commitments attack game, the adversary cannot obtain any knowledge of $k_{\text{shared}}$ from $w$. So, in our fuzzy negotiation structure, biometric values with any entropy can be used to establish shared keys.

We summarize the advantages of our fuzzy negotiation technology as follows. (1) Shared keys are produced by biometric nodes themselves, rather than delivering shared keys from one biosensor node to others, which reduces the messages that need to be delivered in key negotiation. With the help of broadcast mechanism, the method is suitable to establish shared keys among biosensors with more than two nodes. (2) Using two predeployed keys, $k_0$ and $k_1$ to generate shared keys, it helps the key negotiation scheme to withstand the RCB attack with little extra storage cost. (3) Breaking the limit that only high-entropy biometric data could be used to negotiate shared keys and widening the choice of the kinds of biometric data used in the practical negotiation of keys in BSNs.

## 4. Efficient Linear Interpolation Encryption with Keys Sampling Method

In [23], the linear interpolation operation is iteratively executed with interpolation factors and physiological signals to produce cipher text, and the cipher text can hide the physiological signals if interpolation factors keep confidential. However, the scheme does not give the detail on how to generate linear interpolation factors and only claims that these factors can be derived from the session key, which makes INTRAS lacking of operational guidance. In addition, if we use the method in [22] to produce the session keys, the keys may be easily captured by RCB attack according to the description in Section 2.1, which will cause the divulgation of interpolation factors and furthermore the divulgation of physiological signals. To address the problems, in this section we propose a concrete sampling method to generate interpolation factors and then design an efficient INTRAS encryption scheme that can resist RCB attack.

*4.1. The Key Sampling Method.* In this subsection, we propose a key sampling method that can produce a sequence of linear interpolation factors with enough length from the shared key to be used to encrypt biometric data. And the method is described as follows.

Before generating the sequence of interpolation factors, the two parts, A (the sender) and B (the receiver), extend their shared key $k_{\text{shared}}$ to a secret sequence $S$, respectively, using an open hash function $H(\cdot) : S = H(k_{\text{shared}} \| \text{“1”}) \| H(k_{\text{shared}} \| \text{“2”}) \| \cdots \| H(k_{\text{shared}} \| \text{“}n\text{”}) \| \cdots$. We assume $S$ has enough length to encrypt biometric data transferred between A and B.

We call some consecutive bits of $S$ as a sampling window, and before extract interpolation factors from the shared key $k_{\text{shared}}$, we let the sender A produce two secret parameters: open $\ell$ and secret $wn$; therein $\ell$ is the size of sample window; $wn$ is a secret vector: $wn = \langle wn_1, \ldots, wn_z \rangle$, where $wn_i$ $(1 \le i \le z)$ denotes the start position of a sampling window and $z$ is the number of interpolation factors required by encrypting biometric data.

When A needs to extract a sequence of interpolation factors $D$ from $S$, it denotes each interpolation factor $d_i$ by the value of a $S$'s fragment that is with a length of $\ell$ bits and starts from the $wn_i$ bit of $S$. Security here is achieved from the fact that the adversary does not know the distribution of $S$, which renders it infeasible to computer each interpolation factor $d_i$. After producing $D$, A sends $\ell$ and $E_{k_{\text{shared}}}(wn)$ to B, therein $E_{k_{\text{shared}}}(wn)$ means using $k_{\text{shared}}$ to encrypt $wn$ in a symmetric encryption algorithm (such as AES). And then, B can produce the same sequence of interpolation factors.

*4.2. An Improved INTRAS Encryption Scheme.* Using the sequence of interpolation factors $D$, we combine the traditional encryption and signal encryption to propose an improved INTRAS encryption scheme. In the improved scheme, we first encode raw biometric data into a sequence $X$ by PCM (pulse code modulation) encoding, and we then encrypt a fragment of biometric data sequence $X$ using a fragment of $D$ by iterative linear interpolation method. More specifically, we denote a fragment of biometric data

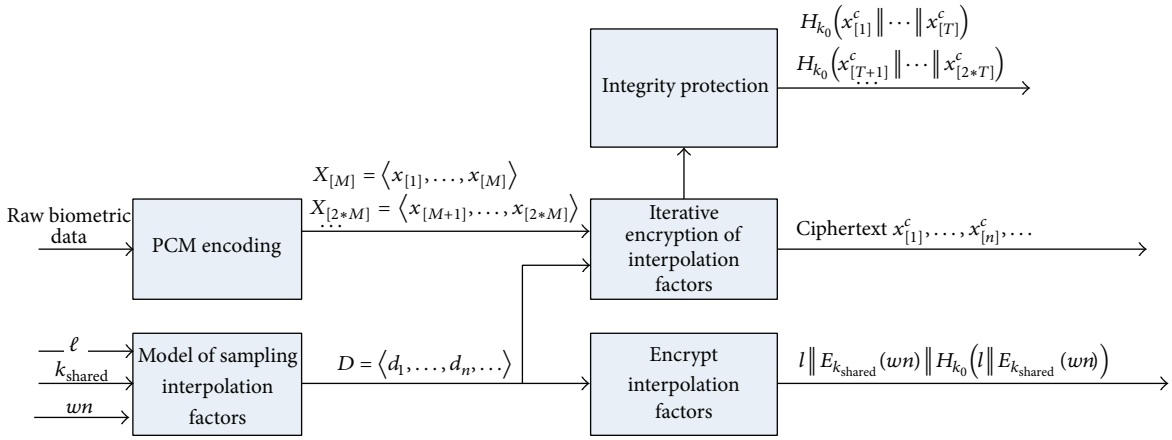


Figure 2: An improved INTRAS encryption.

$\langle x_{[n-M+1]}, \ldots, x_{[n]} \rangle$ $(n \geq M \geq 2)$ as $X_{[n]}$, and we define the two parts of a communication as A and B, where A is the sender and B is the receiver. In addition, assume that $M$ is the number of biometric values in a biometric data fragment, and $T$ is the number of fragments encrypted by a fragment of interpolation factors sequences. If $X_{[n]}$ corresponds to a fragment of $D$ : $D_i = \langle d_{i-M+1}, \ldots, d_i \rangle$ $(i \geq M \geq 2)$, the iterative linear interpolation encryption of $X_{[n]}$ is defined by $x^c_{[n]} = \sum_{j=0}^{M-1} d_{i-j} \cdot x_{[n-j]}$. In addition, when $1 \leq n < M$, we need a secret initiation vector $V = \langle v_1, \ldots, v_{M-1} \rangle$ that is preshared by A and B to encrypt the fragment $X_{[n]} = \langle v_n, v_{n+1}, \ldots, v_{M-1}, x_1, \ldots, x_{[n]} \rangle$, and the encryption is defined as $x^c_{[n]} = \sum_{o=n,i=1}^{M-1,M-n} v_o d_i + \sum_{j=1}^{n} x_{[j]} d_{M-n+j}$. For instance, when $n = 1$, $X_{[1]} = \langle v_1, v_2, \ldots, v_{M-1}, x_1 \rangle$ can be encrypted as $x^c_{[1]} = \sum_{i=1}^{M-1} d_i v_i + x_{[1]} d_M$ $(M \geq 2)$. In the encryption process, if $D_i$ has been used to encrypt $T$ number of biometric data fragments, $X_{n-T+1}, \ldots, X_{n-1}, X_n$ $(T \leq n - M + 1)$, we will use the next fragment of $D$, $\langle d_{i+1}, \ldots, d_{i+M} \rangle$, to encrypt the next $T$ number of biometric data sequences $X_{n+1}, \ldots, X_{n+T}$. In order to protect the integrity of biometric data transferred from A to B, A should use a keyed pseudorandom hash function $H_{k_0}(\cdot)$ to produce a commitment: $H_{k_0}(x^c_{[n-T+1]} \| \cdots \| x^c_{[n-1]} \| x^c_{[n]})$.

Before B decrypts the encrypted messages that is received from A, A must send $\ell$, $E_{k_{\text{shared}}}(wn)$, and $H_{k_0}(\ell \| E_{k_{\text{shared}}}(wn))$ to B; therein $H_{k_0}(\ell \| E_{k_{\text{shared}}}(wn))$ is used to commit the integrity of $\ell$ and $E_{k_{\text{shared}}}(wn)$. When B wants to decrypt biometric data, at first, it checks the integrity of $\ell$ and $E_{k_{\text{shared}}}(wn)$; if the integrity is valid, it will use $\ell$ and $wn$ to produce the same interpolation factors sequence $D$ as A. Next, B will check the integrity of encrypted biometric data, and if the integrity is valid, it will use $D$ and $V$ to decrypt the received encrypted messages by iterative decryption method.

For simplicity, Figure 2 only shows the sender part of the improved INTRAS encryption scheme.

*4.3. Security Analysis.* INTRAS encryption is different from the traditional encryption scheme, and it adopts a simple addition operation and a multiplication operation to hide biometric data, which results in a piece of ciphertext exposing some valuable information about corresponding biometric value. Here we take our improved INTRAS encryption scheme as an example. Suppose in an improved INTRAS encryption scheme $\ell = 10$, $M = 3$, and the range of the biometric values needed to be encrypted was studied in [10, 21]. Thus, if an interpolation factor is 1023 (the maximum value when $\ell = 10$) in a fragment of $D$, the encrypted biometric values produced by the fragment should be between 10230 and 61410. In other words, if an adversary receives an encrypted value between 10230 and 61410, and it also knows $M$ and the range of biometric values, it will induce the value of $\ell$ easily. Thus, in our improved INTRAS encryption scheme, $\ell$ does not need to be encrypted.

Though $\ell$ is open, we argue that the improved INTRAS encryption scheme is still a secure scheme. Below, we will explain this in terms of security of interpolation factors and biometric data, respectively.

*(1) Security of Interpolation Factors.* In the analysis, we consider the worst case where all of biometric values encrypted by a fragment of $D$ are captured by the adversary using RCB attack. And in this context, the adversary will get the following equations set:

$$\begin{aligned} x^c_o &= x_{[o+1-M]} d_u + x_{[o+2-M]} d_{u+1} + \cdots + x_{[o]} d_{u+M-1}, \\ x^c_{o+1} &= x_{[o+2-M]} d_u + x_{[o+3-M]} d_{u+1} + \cdots + x_{[o+1]} d_{u+M-1}, \\ &\vdots \\ x^c_{o+T-1} &= x_{[o+T-M]} d_u + x_{[o+T+1-M]} d_{u+1} \\ &\quad + \cdots + x_{[o+T-1]} d_{u+M-1}. \end{aligned} \tag{2}$$

The above equations set is a linear equation group, where $x_{[o+1-M]}, \ldots, x_{[o+T-1]}$ $(o + 1 \geq M \geq T)$ are known

to the adversary. And by simple calculation, the adversary can get the following equation:

$$Z^c = Z_u d_u + \cdots + Z_{u+M-T} d_{u+M-T}. \quad (3)$$

In the equation, $Z_c$ and the coefficients $Z_u, \ldots, Z_{u+M-T}$ are known by the adversary. Because the length of each interpolation factor is $\ell$ bits, the search space of adversary is $2^{\ell \times (M-T-1)}$ before he guesses the right values of $\langle d_u, \ldots, d_{u+M-T} \rangle$. When $\ell \times (M - T - 1) \geq 128$, the adversary hardly guesses the right fragment of $D$. For instance, if $\ell = 10$ and $T = 2$, then $M$ must be 16. That is, the sender should execute the following encryption:

$$\begin{aligned} x_o^c &= x_{[o-15]} d_u + x_{[o-14]} d_{u+1} + \cdots + x_{[o]} d_{u+15}, \\ x_{o+1}^c &= x_{[o-14]} d_u + x_{[o-13]} d_{u+1} + \cdots + x_{[o+1]} d_{u+15}. \end{aligned} \quad (4)$$

Next, the sender will use $\langle d_{[u+16]}, \ldots, d_{[u+31]} \rangle$ to encrypt $\langle x_{[o-13]}, x_{[o-12]} \ldots, x_{[o+2]} \rangle$ and $\langle x_{[o-12]}, x_{[o-12]} \ldots, x_{[o+3]} \rangle$.

Thus, it can be seen that, in the worst case, the improved scheme still can maintain the security of interpolation factors as long as we give suitable values to $\ell$, $M$, and $T$.

*(2) Security of INTRAS Encryption.* Due to existence of RCB attack, we hardly can resist an adversary to capture some kinds of biometric data remotely, while we should take measures to prevent the adversary from obtaining biometric data which it cannot capture remotely using the information which it can obtain by RCB attack. In the following, we show that the improved INTRAS encryption scheme can maintain the security of biometric data that cannot be captured by RCB attack.

In this analysis, we suppose the interpolation factors sequence $D$ is secure, and then the worst case is that when a fragment of $D$ is used to encrypt $T$ fragments of biometric data, the former $T-1$ numbers of fragments in the $T$ fragments are known to the adversary; then we analyze whether the last value of the $T$th fragment is secure.

According to the above assumption, ciphertext $x_o^c, \ldots, x_{o+T-1}^c$ and biometric data $x_{[o+1-M]}, x_{[o+2-M]}, \ldots, x_{[o+T-2]}$ in the above equations set are known to the adversary. Then, the adversary can get the following equation by calculation:

$$Z^c = Z_{u+T-1} d_{u+T-1} + \cdots + Z_{u+M-2} d_{u+M-2} + Z_{u+M-1} d_{u+M-1}, \quad (5)$$

where $Z^c, Z_{u+T-1}, \ldots, Z_{u+M-2}$ are known to the adversary, $Z_{u+M-1}$ can be defined as $Z_{u+M-1} = Z_a + Z_b x_{[o+T-1]}$, and $Z_a$ and $Z_b$ are also known to the adversary.

Then, $x_{[o+T-1]} = ((Z^c - (Z_{u+T-1} d_{u+T-1} + \cdots + Z_{u+M-2} d_{u+M-2}))/d_{u+M-1} - Z_a)/Z_b$.

Because $d_{u+T-1}, \ldots, d_{u+M-2}, d_{u+M-1}$ are unknown to the adversary, which means the space the adversary needs to search is $2^{\ell(M-T+1)}$, and when $\ell(M - T + 1) \geq 128$, the biometric data which the adversary cannot capture by RCB attack are secure.

In other respects, due to the randomness of interpolation factors, the curve of encrypted data made by the improved INTRAS will hide the original curve of biometric data.

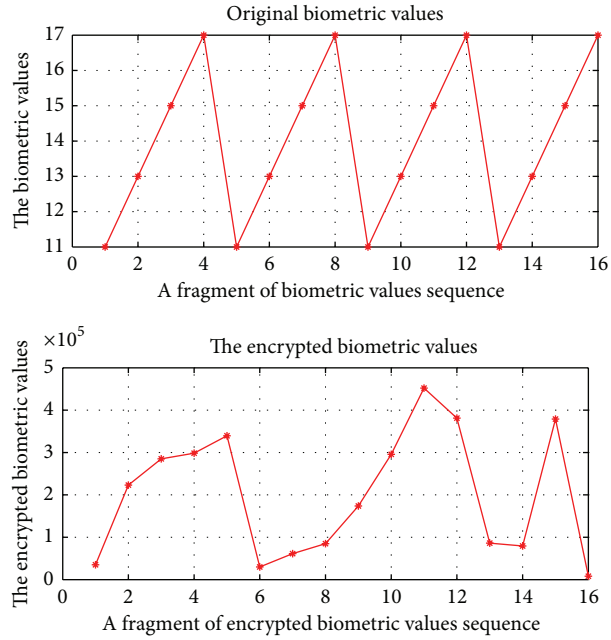


Figure 3: Comparison of original biometric values and encrypted biometric values.

For instance, if $\ell = 10$, $M = 16$, $T = 2$, we use the Matlab tool to simulate the encryption, where initialization vector is randomly produced from range [1, 1023]; the fragment of the biometric data sequence is [11 13 15 17 11 13 15 17 11 13 15 17 11 13 15 17], the interpolation factors are randomly produced from range [1, 1023], and each fragment of interpolation factors sequence is used to encrypt two fragments of biometric data sequence. For instance, the first fragment of interpolation factors sequence is used to encrypt $\langle v_1, \ldots, v_{15}, 11 \rangle$ and $\langle v_2, \ldots, v_{15}, 11, 13 \rangle$, and then, we use next fragment of interpolation factors sequence to encrypt $\langle v_3, \ldots, v_{15}, 11, 13, 15 \rangle$ and $\langle v_4, \ldots, v_{15}, 11, 13, 15, 17 \rangle$ as shown in Figure 3.

From Figure 3 we can see that the improved INTRAS encryption scheme not only can hide the values of biometric values, but also can hide the changing trend of biometric values.

## 5. Conclusion

In order to improve the security of BSNs and provide BSNs with maximum protection from RCB attacks, we propose two improved approaches in this paper. One approach proposes a fuzzy negotiation structure that can use biometric data with any entropy to negotiate shared keys between biosensor nodes. Furthermore, when some shared keys are generated from biometric data that can be threatened by RCB attacks, the structure can secure these keys and also other biometric data that cannot be captured remotely. The second approach firstly proposed a key sampling method, which was not studied in the original INTRAS encryption, and it can be used to produce interpolation factors. We also proposed an

improved INTRAS encryption scheme that can effectively resist the RCB attacks. Security analyses show our approaches are adequate for being used to secure BSNs.

## Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

## Acknowledgments

This work was supported in part by the Open Research Fund from Shandong Provincial Key Laboratory of Computer Network, Grant No. SDKL-2013-05; Jinan Independent Innovation Project (201303013); Shandong Provincial Natural Science Foundation (ZR2011FL027, ZR2012FM005); National Natural Science Foundation (61101162\61101085\60873041\71171122); and "Strategic Priority Research Program" of the Chinese Academy of Sciences (XDA06010701).

## References

[1] G. Xu, Y. Liu, and Y. Xiao, "A secure data transmission scheme for body sensor network," *Journal of Communications*, vol. 8, no. 5, pp. 307–314, 2013.

[2] W. Wang, C. Wang, and M. Zhao, "Resource optimized TTSH-URA for multimedia stream authentication in swallowable-capsule-based wireless body sensor networks," *IEEE Journal of Biomedical and Health Informatics*, vol. 18, no. 2, pp. 404–410, 2014.

[3] C. Otto, A. Milenkovic, C. Sanders, and E. Jovanov, "System Architecture of a wireless Body Area Sensor Network for Ubiquitous Health Monitoring," *Journal of Mobile Multimedia*, vol. 1, no. 4, pp. 307–326, 2005.

[4] S. H. Cheng and C. Y. Huang, "Coloring-based inter-WBAN scheduling for mobile wireless body area networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 2, pp. 250–259, 2013.

[5] L. Shi, J. Yuan, S. Yu, and M. Li, "ASK-BAN: authenticated secret key extraction utilizing channel characteristics for Body Area Networks," in *Proceedings of the 6th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '13)*, pp. 155–166, Budapest, Hungary, April 2013.

[6] E. Jovanov, A. Milenkovic, C. Otto, and P. C. De Groen, "A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation," *Journal of Neuro-Engineering and Rehabilitation*, vol. 2, no. 6, pp. 1–10, 2005.

[7] G. Z. Yang, *Body Sensor Networks*, Springer, London, UK, 1st edition, 2006.

[8] J. Hu, H.-H. Chen, and T.-W. Hou, "A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations," *Computer Standards & Interfaces*, vol. 32, no. 5-6, pp. 274–280, 2010.

[9] W. D. Yu and M. A. Chekhanovskiy, "An electronic health record content protection system using SmartCard and PMR," in *Proceedings of the 9th International Conference on e-Health Networking, Application and Services*, pp. 11–18, June 2007.

[10] HIMSS Reports, "Systemic Interoperability Commission Releases Report to Congress and Administration," 2005, http://www.himss.org/ASP/topicsNewsitem.asp?cid=65448&tid=3.

[11] W. B. Lee and C. D. Lee, "A cryptographic key management solution for HIPAA privacy/security regulations," *IEEE Transactions on Information Technology in Biomedicine*, vol. 12, no. 1, pp. 34–41, 2008.

[12] T. Kwon and J. Hong, "Secure and efficient broadcast authentication in wireless sensor networks," *IEEE Transactions on Computers*, vol. 59, no. 8, pp. 1120–1133, 2010.

[13] R. di Pietro, L. V. Mancini, C. Soriente, A. Spognardi, and G. Tsudik, "Data security in unattended wireless sensor networks," *IEEE Transactions on Computers*, vol. 58, no. 11, pp. 1500–1511, 2009.

[14] A. S. Uluagac, R. A. Beyah, and J. A. Copeland, "Secure SOurce-BAsed Loose Synchronization (SOBAS) for wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 4, pp. 803–813, 2013.

[15] A. Rasheed and R. N. Mahapatra, "The three-tier security scheme in wireless sensor networks with mobile sinks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 5, pp. 958–965, 2012.

[16] T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," *IEEE Transactions on Mobile Computing*, vol. 9, no. 7, pp. 941–954, 2010.

[17] Y. Chen and W. T. Tsai, *Service-Oriented Computing and Web Software Integration*, Kendall Hunt, 4th edition, 2014.

[18] Y. Wang, J. Hu, and D. Philip, "A fingerprint orientation model based on 2D Fourier Expansion (FOMFE) and its application to singular-point detection and fingerprint Indexing," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 573–585, 2007.

[19] F. Sufi, I. Khalil, and J. Hu, "ECG based biometric identifications," in *Springer Handbook of Information and Communication Security*, Springer, New York, NY, USA, 2010.

[20] K. Xi and J. Hu, "Bio-cryptography," in *Handbook of Information and Communication Security*, pp. 129–157, Springer, Berlin, Germany, 2010.

[21] K. Xi, T. Ahmad, F. Han, and J. Hu, "A fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobile computing environment," *Journal of Security and Communication Networks*, vol. 4, no. 5, pp. 487–499, 2011.

[22] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proceedings of the 6th ACM Conference on Computer and Communication Security (CSS '99)*, pp. 28–36, November 1999.

[23] F. M. Bui and D. Hatzinakos, "Biometric methods for secure communications in body sensor networks: Resource-efficient key management and signal-level data scrambling," *Eurasip Journal on Advances in Signal Processing*, vol. 2008, Article ID 529879, 2008.

[24] S. Cherukuri, K. K. Venkatasubramanian, and S. K. S. Gupta, "Biosec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," in *Proceedings of the 32nd International Conference on Parallel Processing (ICPP '03)*, pp. 432–439, October 2003.

[25] S. Mesmoudi and M. Feham, "BSK-WBSN: biometric symmetric keys to secure wireless body sensors networks," *International Journal of Security and Its Applications*, vol. 3, no. 5, pp. 155–166, 2011.

[26] K. K. Venkatasubramanian and S. K. S. Gupta, "Security for pervasive health monitoring sensor applications," in *Proceedings of the 4th International Conference on Intelligent Sensing and*

*Information Processing (ICISIP '06)*, pp. 197–202, December 2006.

[27] S. D. Bao, L. F. Shen, and Y. T. Zhang, "A novel key distribution of body area networks for telemedicine," in *Proceedings of the IEEE International Workshop on Biomedical Circuits and Systems*, pp. 1–11, December 2004.

[28] H. Zhao, J. Qin, and J. Hu, "An energy efficient key management scheme for body sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 11, pp. 2202–2210, 2013.

[29] K. Cho and D. H. Lee, "Biometric based secure communications without pre-deployed key for biosensor implanted in body sensor networks," *Lecture Notes in Computer Science*, vol. 7115, pp. 203–218, 2012.

[30] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: how to generate strong keys from biometrics and other noisy data," in *Advances in Cryptology—EUROCRYPT 2004*, pp. 523–540, Springer, Berlin, Germany, 2004.

[31] X. Boyen, "Reusable cryptographic fuzzy extractors," in *Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS '04)*, pp. 82–91, October 2004.

[32] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractor: a brief survey of results from 2004 to 2006," in *Security with Noisy Data*, chapter 5, Springer, Heidelberg, Germany, 2007.

[33] K. Simoens, P. Tuyls, and B. Preneel, "Privacy weaknesses in biometric sketches," in *Proceedings of the 30th IEEE Symposium on Security and Privacy*, pp. 188–203, Berkeley, Calif, USA, May 2009.

[34] M. Blanton and M. Aliasgari, "On the (non-)reusability of fuzzy sketches and extractors and security in the computational setting," in *Proceedings of the International Conference on Security and Cryptography (SECRYPT '11)*, pp. 68–77, July 2011.

[35] Y. Dodis, B. Kanukurthi, J. Katz, L. Reyzin, and A. Smith, "Robust fuzzy extractors and authenticated key agreement from close secrets," *IEEE Transactions on Information Theory*, vol. 58, no. 9, pp. 6207–6222, 2012.