Efficient Secret Key Delivery Using Heartbeats

Kwantae Cho[1,*], and *Byungho* Chung[2]

[1, 2] Information Security Research Division, Electronics and Telecommunications Research Institute, Republic of Korea

Abstract. Recently many researchers have employed physiological signals like heartbeats as a source of the key seed used in key establishment protocols. The physiological signals make it easy to establish a secret key between implantable (or attachable) medical devices which can sense physiological signals. A key establishment protocol is a fundamental requirement to support the security of the healthcare and medical services such as diagnosis, treatment, prevention, and follow-up services. However, existing key establishment protocols demand high computational and communication costs or need long key establishment time. In this paper, we propose an efficient IPI-based key establishment protocol that requires relatively short time while keeping the strength of security close.

1 Introduction

Recent advances of sensor technologies have enabled the emergence of small types of sensor devices, especially, called biometric sensors. Generally, biometric sensors are small enough and they can be attached on or implanted in the human body in order to monitor physiological signals. Once integrated with wireless network modules, biometric sensors can construct a special kind of wireless sensor networks in a human body, called as body sensor networks (BSNs). The biometric sensors check the health status of the human body and, as needed, they may carry out intelligent treatment via their mutual communication automatically. The information covered by BSNs not only involves individual privacy, but it may even be life threatening in the worst case. For example, if an attacker with malicious intent can control the insulin injector implanted in a particular patient at will and it excesses insulin into the patient's body, the patient will be in a very dangerous situation. Thus, privacy and security protection of the BSNs is an essential requirement to popularize medical and healthcare services.

In BSNs, the use of biometrics, specifically, physiological signal, makes it possible to provide stronger security more easily. We can imagine that a long-term secret key is embedded in implantable medical devices before deployment. If a malicious attacker gets the long-term key by unpredicted accidents or a compromise attack, the patient with the implantable medical device will have to undergo surgery to update the long-term secret key. If asymmetric cryptosystem is applied to the implantable medical device, it may not be necessary to store the secret key in advance, but it will bring a huge energy problem to the medical device. For these reasons, many security researchers have proposed symmetric key-based cryptographic protocols that does not required storing secret information in advance.

Most of physiological-signal-based key establishment schemes [1-6] have been designed based on fuzzy-vault scheme [7]. However the fuzzy-vault scheme fundamentally requires significant computation and communication costs by a number of polynomial calculations and the transmission of numerous chaff points. For these reasons, most researchers have tried to deal with the issues. The work [3] reduced computational costs by not calculating lagrangian interpolation coefficients only by transmitting matched points to the other party. The work [4] employs simple arithmetic operators instead of Euclidean distance formula which requires squaring and square root, for vault unlocking. Above these, the works [5-6] have been enhanced the security of fuzzy-vault. In the works, chaff points are chosen from not 1-dimensional space but 2-dimensional space in order to increase the number of available points and make it difficult for a brute force attack to be successful.

In this paper, we propose a lightweight key establishment scheme using inter-pulse interval (IPI) of photoplethysmogram (PPG), in order to avoid the above disadvantages of the fuzzy-vault scheme. Here, an IPI means the interval between two peaks of the PPG signals. If the IPIs are used for key establishment scheme, it is not necessary to derive the polynomial, unlike the fuzzy-vault, and there is no need to transmit chaff points, so the amount of computation and the amount of traffic can be greatly reduced. Although various IPI-based key establishment schemes [8-12] have been proposed so far, the work [13] recently proposed a simple and efficient IPI-based key delivery protocol. The work [13] encodes the secret key generated by biometric sensor A using an error correction code (ECC), then A hides it in a witness, which is generated from the biometric information measured by itself, and transmits it securely to another biometric sensor B. Then B recovers the secret key using its own witness. However, since the work has to collect

* Corresponding author: kwantaecho@etri.re.kr

biometric information for witness generation as long as the bit length of the encoded output, the secret key exchange takes a relatively long time.

In this paper, we have reduced the key generation time by lessening the length of witness, while maintaining the advantages of the IPI-based key establishment schemes. Biometric sensor *A* encodes the generated witness using the ECC and it transmits only the parity code of the encoded outputs to another biometric sensor *B*. Also, in order to hide a secret key in the witness, A needs a witness equivalent to the key length, not the encoded output length. The main contributions of the paper are outlined as follows.

1) *Relatively short key establishment time:* we shortened the key establishment time by reducing the number of IPIs needed to generate a secret key. It will be possible to access the medical device (biometric sensor) faster in an emergency.
2) Low *computational and communication cost:* The proposed protocol adopts a symmetric cryptosystem, not an asymmetric cryptosystem. Furthermore, the proposed protocol does not transmit a large amount of data like chaff points of the fuzzy-vault.

The remainder of this paper is organized as follows. Section 2 introduces backgrounds of the proposed key delivery protocol. After explaining our IPI-based key delivery protocol in Section 3, we discuss the performance of the proposed protocol in Section 4. Finally, we conclude this paper in Section 5.

2 Backgrounds

In this section, we explain our system and adversary models, and we briefly introduce related works.

2.1. Overview of System model

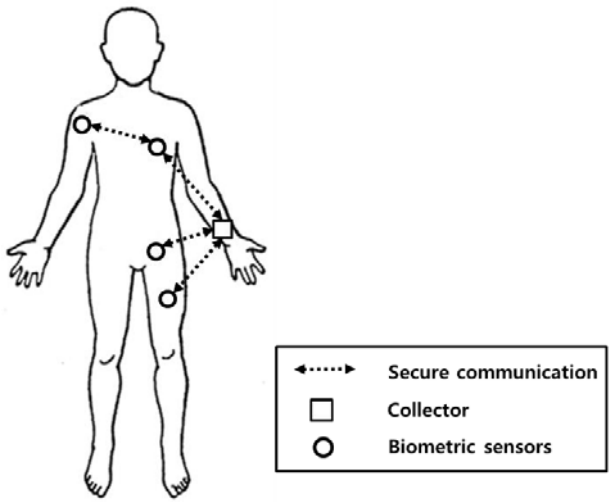

Fig. 1. Our System Model

Fig. 1 depicts our system model, which can be applied to biometric-based systems such as u-Healthcare service system, a BSN (a Body Sensor Networks), and a WBAN (a Wireless Body Area Network). Such systems are mainly made up of two types of devices: a Collector and several biometric sensors. Each biometric sensor can be attached to a body or implanted in the body as necessary. The collector can be wirelessly connected to an external management server. Each biometric sensor measures biometric information of the body for various tasks such as health status monitoring and medical decision support, while offering the biometric information to the collector. The collector periodically aggregates the biometric information from each biometric sensor installed in the same body, and then it sends the aggregated data to the external management server.

In our system model, the collector as well as the biometric sensors can measure the inter-pulse interval (IPI) of the photoplethysmogram (PPG). Here, IPIs can be measured in / above the human body [14]. In biometric-based systems, since biometric sensors handle private medical information of patients, it is necessary to construct secure communication between them. The secret key delivery protocol, which proposed in this paper, allows two biometric sensors (or between a biometric sensor and a collector) to share a secret key for secure communication between themselves.

2.2. Adversary model

The type of an adversary *A* can be divided into two types as follows. The first is to find who possess a certain biometrics even though *A* does not have any secret which is shared between a collector and each biometric sensor and used in process of authentication. The second is to make a valid response even though *A* is not a legitimate participant. More specifically, *A* wants to be not only authenticated by a collector or biometric sensors of the attack target, but also participate in a secret delivery protocol by pretending to be a legitimate participant. Accordingly, we can define two adversary types: a *passive adversary* and an *active adversary*.

A passive adversary is an adversary that can just eavesdrop and collect the exchanged messages between legitimate participants but cannot inject and modify their messages because *A* has no ability to make a valid challenge and response of the secret key delivery protocol. For instance, tracing through continuous eavesdropping is one of passive attacks. Meanwhile, an active adversary is defined as *A* who can fabricate messages and insert them into the normal authentication process to achieve his/her malicious purpose. Here, we assume that an active adversary cannot physically access a biometric sensor because physical access to a biometric sensor implanted in a body or attached on a body is quite difficult. The attack target will probably be able to easily recognize the physical access. For example, impersonation and spoofing attacks belong to this attack.

2.3. Related works

The feasibility of IPIs for key establishment between biometric sensors have been studied steadily. It relies heavily on the randomness of IPIs and their disparity between IPIs obtained by different subjects. In this

subsection, we discuss these IPI characteristics and then we introduce some of the representative IPI-based key delivery protocols.

In many previous works [8-12], it is already evaluated that each IPI, which is obtained from healthy subjects as well as patients with cardiovascular diseases, has a high degree of entropy and it therefore can be used as a security key. However, all bits of an IPI does not have a high degree of entropy. Although the length of IPIs is from eight to ten bits in accordance with the sampling rate of a biometric sensor and each IPI is time-variant, it is known that only the three or four least-significant bits (LSBs) of all its bits are independent random variables [12-13].

One of the most important consideration when IPIs are used for key establishment is the disparity between IPIs which are simultaneously obtained from the same body. Most related works [13, 15-17] have focused on how to efficiently synchronize IPIs having such a property. The work [15] firstly proposed the key establishment scheme using IPIs while the works [16] and [17] did not share any secret information between two parties in advance for key exchange. Compared with these works, the work [13] does not use pre-deployed secret information while reducing the number of communication rounds considerably.

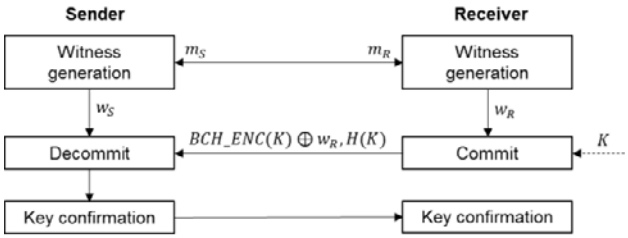

Fig. 2. Outline of the work [13]

Fig. 3 shows the outline of the work [13]. It is assumed that two biometric sensors (Sender and Receiver) are attached to the same subject. Both biometric sensors measure IPIs in real time and they periodically exchange misdetection flag (m_S, m_R) for the block consisting of several trimmed IPIs. The sender and the receiver generate witness values (w_S and w_R, respectively) generated from the blocks. The receiver creates nonce K used as a symmetric key between itself and the sender. After encoding the nonce using the BCH (Bose–Chaudhuri–Hocquenghem) code, the receiver computes XOR operation with the encoded codes and its witness w_R, and then it transmits the computed results to the sender. The sender runs XOR operation with the received value and its witness w_S, decodes the encoded codes. Finally, the sender checks whether a derived key is correct through the key confirmation step. However, the work [13] requires a relatively long time to exchange a secret key. For example, it takes between 60 and 77.6 seconds to generate a 80-bit key with using three LSBs and (204, 80, 37) BCH codes; that is, a 204-bit witness is required to make a 80 bit key and it is derived from about 68 IPIs. The key-exchange time should be reduced for practical use. In this paper, we significantly reduced the expected key-exchange time by modifying the commit step effectively.

3 Proposed secret key delivery protocol

In this section, we explain the proposed secret key deliver protocol between two biometric sensors (a Sender and a Receiver) using IPIs. The proposed protocol is composed of several steps: witness generation, ECC encoding & decoding, key generation, key transmission, key derivation, key verification, and key confirmation. The three steps (ECC encoding, key generation, and key transmission) accord with the Commit step of Fig. 2 while other three steps (ECC decoding, key derivation, and key transmission) accord with the Decommit step of that. Fig. 3 depicts our proposed secret key deliver protocol. The notation is shown in Table 1.

Table 1. Notation

Notation	Description
n	The number of IPIs (or witnesses) needed to generate a key
IPI_i	The i-th of n IPIs
$w_{x,i}$	The i-th witness piece of biometric sensor x
w_x	Witness of biometric sensor x
BCH_ENC / BCH_DEC	Normal In brackets
P	Parity code of the encoded output using BCH code
K	A symmetric session key between Sender and Receiver
TS	Timestamp
$MAC_K(M)$	A message authentication code to authenticate message M with key K
$\oplus$	A XOR operator
$X \parallel Y$	The concatenation of X and Y
SUCCESS	A flag to mean that a pairwise key between Sender and Receiver is established successfully

3.1. Witness generation

Each biometric sensor makes its own witness from its own measured IPIs in this step. Sender S consecutively measures n IPIs (IPI_1, IPI_2, …, IPI_n), each of which is the time difference between two sequential heartbeats. Like the work [13], we assume that only three LSBs of each IPI is used to produce a witness piece. The selected IPI bits are reprocessed through the Gray coding, which can lower the disparity between two IPIs. We then call the Gray-coded bits as a *witness piece*, i.e., an IPI is a source of a witness piece and n witness pieces ($w_{S,1}, w_{S,2}, \ldots\ldots, w_{S,n}$) become a witness ($w_S$). In the same way as S, Receiver R also generates its own witness w_R (where $w_S \approx w_R$), providing a basis for trust establishment.

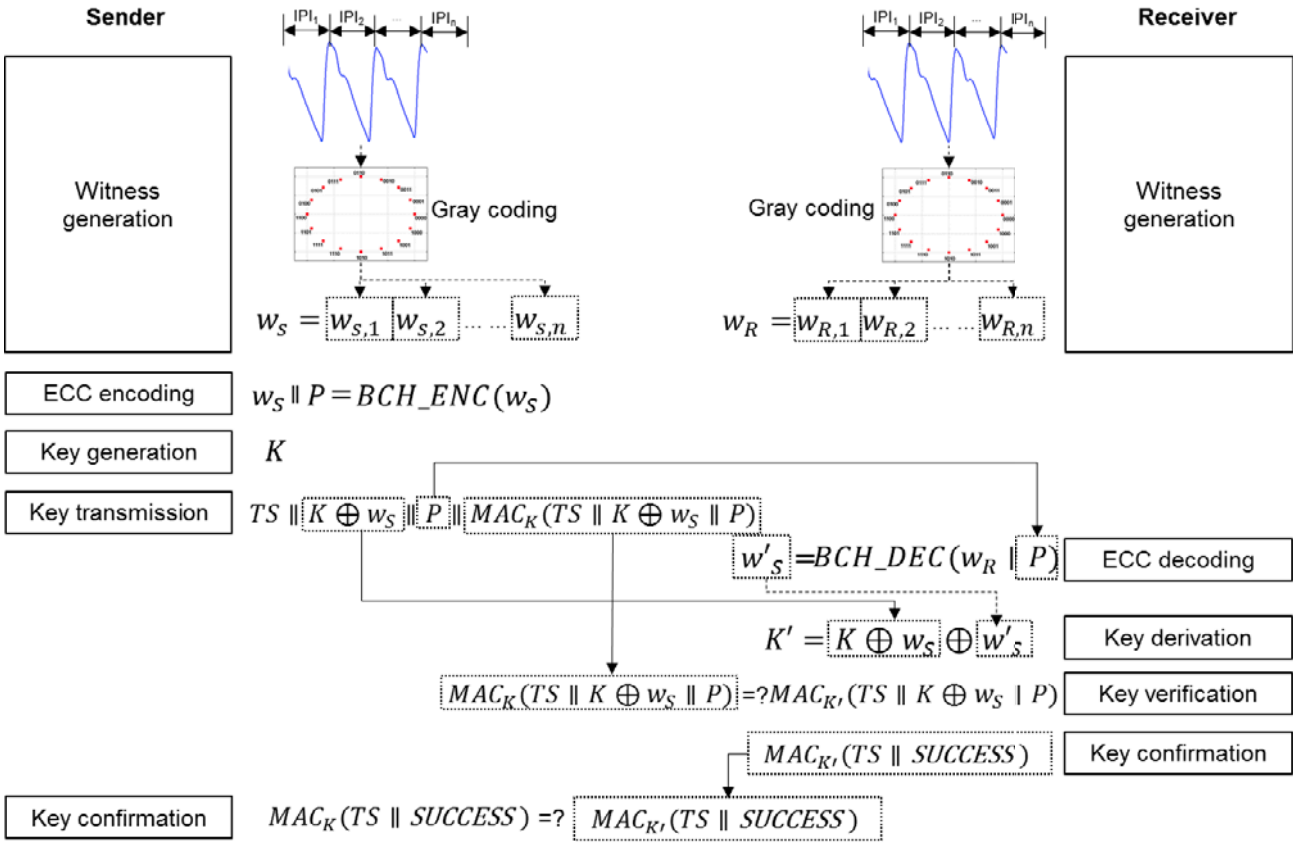

Fig. 3. Proposed key delivery protocol

3.2. ECC encoding & decoding

In this step, S generates parity code P for its w_S using an error correcting code. We employ an error correcting code as the BCH code. The encoded output of the BCH code is separated into its original data w_S and its parity code P. In the key transmission step, only P is sent to R for BCH decoding.

3.3. Key generation & transmission

S generates a secret key and then it provides R with supplementary information required for key derivation and key verification. S selects a nonce used as a symmetric session key K between itself and R. After computing supplementary information $TS \| K \oplus w_S \| P \| MAC_K(TS \| K \oplus w_S \| P)$, S sends R the computed result, which helps R to the end that R recovers the K.

3.4. Key derivation & verification

R derives the same key K using its own witness w_R. On receiving the supplementary information, R decodes it using w_R together with P. Consequently, R can obtain w'_S $(= w_S)$. If the bit difference between w_S and w_R is within the correctable range of the BCH code, w'_S and w_S will be exactly the same. Using w'_S, R computes $K \oplus w_S \oplus w'_S$ and it finally get secret key $K'(= K)$.

For the validation check of K', after calculating $MAC_{K'}(TS \| K \oplus w_S \| P)$, R checks whether the calcaulted result is equal to the received value $MAC_K(TS \| K \oplus w_S \| P)$. If same, R determines K' as a session key during the session associated with S.

3.5. Key confirmation

S confirms that S and R has the identical session key. In this step, R computes $MAC_{K'}(TS \| SUCCESS)$ using its own session key K' and then transmitting it to S. On receiving it, S computes $MAC_K(TS \| SUCCESS)$ and it then checks whether the computed value and the received value are the same. If same, S and R begin secure communication using the session key. Otherwise, they start the entire steps again.

4 Discussion

In this section, we discuss the performance of the proposed key delivery protocol through the comparison with the representative existing work [13]. Fig. 4 compares the security strength between the proposed protocol and the protocol in the existing work. The security strength of the existing work is always the same as the generated key length, that is $2^{-80} (\approx 8.2718 \times 10^{-25})$. However, the security strength of the proposed

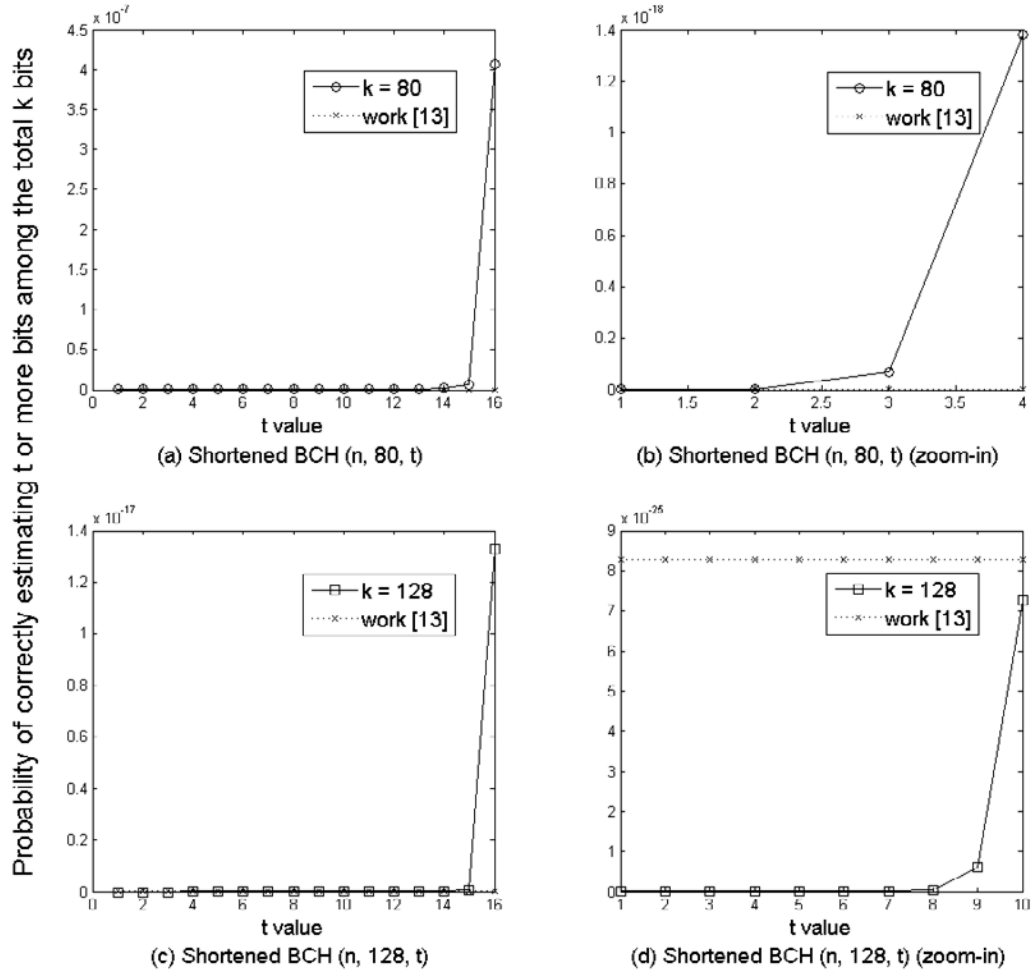

Fig. 4. Key extimation probability according to *t* and a key length

protocol depends on the parameter value, specifically, *k* and *t,* of the BCH code (*n, k, t*); here, *n* is the total bit length of the BCH-encoded data, *k* is the bit length of the BCH input data, and *t* is the number of correctable bits.

In order to get some profitable information, a passive or active adversary should find out a valid session key or guess it accurately. Since it is very difficult for the adversary to directly obtain the biometric information from the body of the attack target, the adversary has to predict the key without a given biometric information. If the adversary can precisely estimate (*k-t*) bits or more, then he/she get a valid session key. Accordingly, we can compute the probability (*P*) of correctly estimating (*k* - *t*) bits ore more among the total *k* bits as below,

$$P = \sum_{i=k-t}^{k} {}_k C_i \left(\frac{1}{2}\right)^k. \quad (1)$$

Fig. 4 stands for the key prediction probability according *k* and *t* in the proposed protocol and the existing protocol. Figs. 4(b) and 4(d) are enlarged versions of Figs. 4(a) and 4(c), respectively. As shown in Figs. 4(a) and 4(b), when k = 80, the key prediction probability is higher in the proposed protocol than in the work [7] at all *t* values. However, in case that k = 128 and t ≤ 10, the key prediction probability of the proposed protocol is lower than that of the existing work. Besides, as the error correction rates of the proposed protocol and the existing protocol are about 0.078 and 0.088, respectively, they are almost similar.

Next, let's look at the key generation time. We assume that 3-bit IPIs are used for a key generation and 70 IPIs are measured per a minute. A 128-bit key for the proposed protocol requires 36.57 secs ($=\frac{128}{3}\times\frac{60}{70}$), while a 80-bit key for the existing protocol needs 58.28 secs ($=\frac{204}{3}\times\frac{60}{70}$). As already expected, the proposed protocol can significantly reduce the key establishment time, compared with the existing protocol, by approximately 35%.

5 Conclusion

In this paper, we proposed an efficient key delivery protocol. Compared to the existing work, we have significantly reduced key generation time by decreasing the size of the witness required to generate a secret key. This advantage will enable faster response by reducing the time to access a secure medical device in an emergency.

In the near future, we will perform real-time testing using actually measured photoplethysmogram in order to investigate the availability of the proposed protocol. Furthermore, we will demonstrate how high probability that a session key between two biometric sensors is established on a simulator to be built in the near future.

Acknowledgements

This work was supported by the ICT R&D program of MSIP/ IITP[2016-0-00575-002, Feasibility Study of Blue IT based on Human Body Research]

References

1. K. K. Venkatasubramanian, A. Banerjee, S. K. S. Gupta, *PSKA: Usable and Secure Key Agreement Scheme for Body Area Networks*, IEEE Trans. Information Technology in Biomedicine (2010)
2. N. Jammali, L. C. *Fourati, PFKA: A Physiological Feature based Key Agreement for Wireless Body Area Network*, International Conf. Wireless Networks and Mobile Communications (2015)
3. C. Hu, X. Cheng, F. Zhang, D. Wu, X. Liao, D. Chen, *OPFKA: Secure and Efficient Ordered-Physiological-Feature-based Key Agreement for Wireless Body Area Networks*, IEEE INFOCOM, pp. 2274-2282 (2013)
4. M. Khalil-Hani, R. Bakhteri, *Securing Cryptographic Key with Fuzzy Vault based on a new Chaff Generation Method*, International Conf. High Performance Computing and Simulation (2010)
5. Y. Lu, S. Bao, *Efficient Fuzzy Vault Application in Node Recognition for Securing BSNs*, IEEE International Conf. Communications (2014)
6. Y. Lu, S. Bao, M. Chen, R. Jin, *Fuzzy Vault Based Automatic Secret Sharing in BSNs*, International Conf. Biomedical Engineering and Informatics (2013)
7. A. Juels, M. Sudan, *A Fuzzy Vault Scheme*, Designs, Codes and Cryptography (2006)
8. C. C. Poon, Y. T. Zhang, S. D. Bao, *A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health*. IEEE Commun. Mag., pp. 73–81 (2006)
9. S. D. Bao, C. C. Y. Poon, Y. T. Zhang, *Using the timing information of heartbeats as an entity identifier to secure body sensor network*, IEEE Trans. Information Technology in Biomedicine, **12**, pp. 772-779 (2008)
10. G. H. Zhang, C. C. Y. Poon, Y. T. Zhang, *Analysis of using interpulse intervals to generate 128-bit biometric random binary sequences for securing wireless body sensor networks*, IEEE Trans. Information Technology in Biomedicine, **16**, pp.176-182 (2012)
11. G. H. Zhang, Y. X. Zhang, Y. T. Zhang, A Comparison of Binary Number Generators for Wireless Body Sensor Networks Security, IEEE-EMBS International Conf. Biomedical and Health Informatics (BHI), pp.782-784 (2012)
12. M. Rostami, A. Juels, F. Koushanfar, *Heart-to-heart (H2H): authentication for implanted medical devices*, ACM CCS, pp. 1099–1112 (2013)
13. R. M. Seepers, J. H. Weber, Z. Erkin, I. Sourdis, C. Strydis, *Secure Key-Exchange Protocol for Implants Using Heartbeats*, ACM International Conf. Computing Frontiers, pp. 119-126 (2016)
14. C. Y. P. Carmen, Z. Yuan-Ting, B. Shu-di, *A Novel Biometrics Method to Secure Wireless Body Area Sensor Networks for Telemedicine and M-Health, IEEE Communications Magazine*, pp. 73-81 (2006)
15. S. Cherukuri, K. K. Venkatasubramanian, S. K. S. Gupta, *BioSec: A Biometric Based Approach for Securing Communication in Wireless Networks of Biosensors Implanted in the Human Body*, International Conf. Parallel Processing Workshops (2003)
16. K. Cho, D. H. Lee, *Biometric Based Secure Communications without Pre-deployed Key for Biosensor Implanted in Body Sensor Networks*, International Workshop on Information Security Applications, pp.203-218 (2011)
17. K. Cho, B. Chung, *Lightweight Biometric Key Agreement Scheme for Secure Body Sensor Networks*, International Journal of Communications, **1**, pp.218-222 (2016)