Lightweight Biometric Key Agreement Scheme for Secure Body Sensor Networks

Kwantae Cho, Byungho Chung
Information Security Research Division
Electronics and Telecommunications Research Institute
218, Gajeong-ro, Yuseong-gu, Daejeon
Republic of Korea
kwantaecho@etri.re.kr, cbh@etri.re.kr

Abstract: A biometric sensor device is the potential product of the forthcoming biotechnology for real-time tracking of physiological signals to support various healthcare and medical services such as homecare medical service, prevention, diagnosis, and follow-up services. A key agreement scheme between biometric sensor devices is a fundamental requirement to support the security of the healthcare and medical services. Existing key agreement schemes employ high computational cryptography mechanisms or share a pre-deployed key among biometric sensor devices. Due to stringent constraints of hardware capability, it is inadequate to use public cryptography mechanisms for biometric sensor devices. Moreover, it is also inappropriate to install a fixed secret key in implanted devices because, if the key is revealed, a person will have inevitable transplantation surgery for the secret redistribution. In this paper, we propose new lightweight key agreement scheme which requires only symmetric cryptosystem without a pre-deployed secret information for biometric sensor devices.

Key–Words: key agreement, biometric key, secure communication, interpulse interval

1 Introduction

The convergence of healthcare and IT technology has assisted the advances of modern medical services such as medical devices implanted in the human body, and remote health monitoring and transmission using healthcare devices. Such biometric sensor devices have made it possible to periodically and automatically manage physical conditions of patients to be concerned. The biometric sensor device carries vital physiological information, thus privacy and security become important challenges in this area for the smooth functioning of medical and healthcare services.

Many kinds of security mechanisms have been applied to the medical and healthcare services. The use of biometrics among the security mechanisms makes it easier and more convenient to serve the high-quality security to the healthcare environments. However, in case of immutable biometrics (e.g., fingerprints, irises, and faces), once the biometrics are compromised, they cannot be replaced or changed. There were two recent reports where hackers stole 5.6 million of irrevocable fingerprints of United States federal employees [1], and implantable medical devices are significantly vulnerable to hacking [2, 3]. In addition, we can imagine that the secret key embedded in implantable medical devices could be revealed by unpredicted accidents or a compromise attack by an adversary. As each biometric device implanted inside the body has pre-deployed key as a secret and the key is revealed, the device user should undergo a operation to renew the pre-deployed key.

In order to avoid danger due to the expose of the immutable biometrics, many researchers have studied various key agreement schemes using ever-changing biometrics such as photoplethysmogram (PPG), electrocardiogram (ECG), and electroencephalogram (EEG). In the existing key agreement schemes, even though an adversary acquires biometrics at a specific time, he/she cannot acquire any sensitive information except for the specific time. However, the existing schemes have some issues requiring high computational cost [4, 5, 6, 7] or storing secret information in biometric devices [8, 9, 10].

In this paper, we introduce new lightweight biometric key agreement scheme on the basis of symmetric cryptosystem without the pre-deployment of secret information. For seed synchronization of session keys, the existing schemes [4, 5, 6, 7] need a lot of computational operations, while the proposed scheme demands fairly low computational operations by utilizing intersection elements between the outputs of bloom filters [11]. Additionally, we demonstrate that the false-positive probability of the proposed scheme

is extremely tiny.

The remainder of this paper is organized as follows. Section 2 introduces our system model and a bloom filter. In Section 3, we explain our lightweight biometric key agreement scheme together with the false-positive probability. Finally, we conclude this paper in Section 4.

Contributions. Our Contributions are as follows:

- *None of pre-deployed secret information* forestalls the undesirable problems caused by the disclosure of secret information.
- *Low computation cost* based on symmetric cryptosystem used in the proposed scheme can comparatively extend the battery life of the biometric sensor devices, specifically, implanted medical devices.

2 Our Preliminaries

2.1 System Model

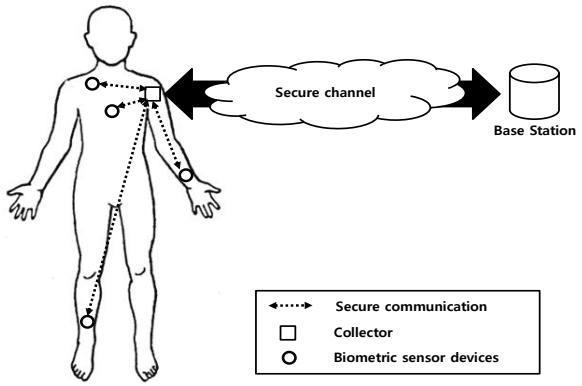

Figure 1: Our System Model

Fig. 1 describes our system model, namely, our concept of BSNs. BSNs consist of three types of devices: a collector on a body, several biometric sensor devices on a body or implanted in a body, and a base station. A collector is connected to a remote base station. Each biometric sensor conducts various operations such as measuring biometrics, processing them, and delivering them to the collector. The collector periodically aggregates biometrics and then it transmits the aggregated data to the base station, by which it is accumulated for service delivery such as monitoring health status of patients.

In our system model, the collector and the biometric sensor devices all together can measure interpulse interval (IPI) of photoplethysmograms (PPGs). The collector is located on the human body and it also measures IPI, which can be also found in/on the human body [12]. The implanted biometric sensor devices measure biometrics more than two kinds of biometrics. The devices measure IPI for establishing a session key with the collector and measure other biometrics which the collector requires. Here, we employ a bloom filter technique [11] for a session key synchronization between a biometric sensor and the collector device. After encrypting the required biometric information using the session key, the biometric sensor devices can transmit the encrypted data to the collector.

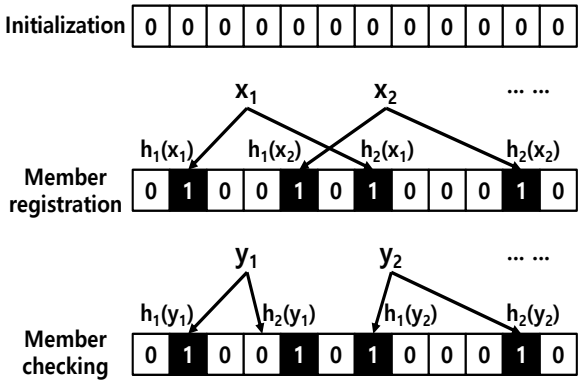

Figure 2: Example of a bloom filter ($m = 12,\ k = 2$).

Generally, a bloom filter is employed for membership checking. It represents n members as a group $G = \{x_1, x_2, \cdots, x_n\}$ and it consists of m bits, initially all set to zero. The bloom filter is based on k independent one-way hash functions $h_1, \cdots, h_k$ having range $\{1, \cdots, m\}$, respectively. For mathematical convenience, we make assumption that the k hash functions map each member in the group to a random uniform over the range $\{1, \cdots, m\}$. For each member $x \in G$, the bits $h_i(x)$ between 1 and m are set from zero to one for $1 \leq i \leq k$. A position can be set to one several times up to k times, but only the first change can be affected. To check whether member y belongs to G, we should confirm that all $h_i(y)$ are set to one. If any of $h_i(y)$ is zero, then definitely y is not in G. If all $h_i(y)$ are set to one, we infer that y is a member of G, even though the inference may be wrong with small probability. Therefore, a bloom filter may cause a *false-positive error*, whereby it can imply that a member x is in G even though it is not.

As shown in Fig. 2 which depicts an example of a bloom filter, the bloom filter can be composed of three phases. In the initialization phase, the bloom filter initializes all bits to zero. During member registration, each member x_i in the group G is hashed k times, resulting in that each hash value yields a bit position; these bits are set to one. During member checking,

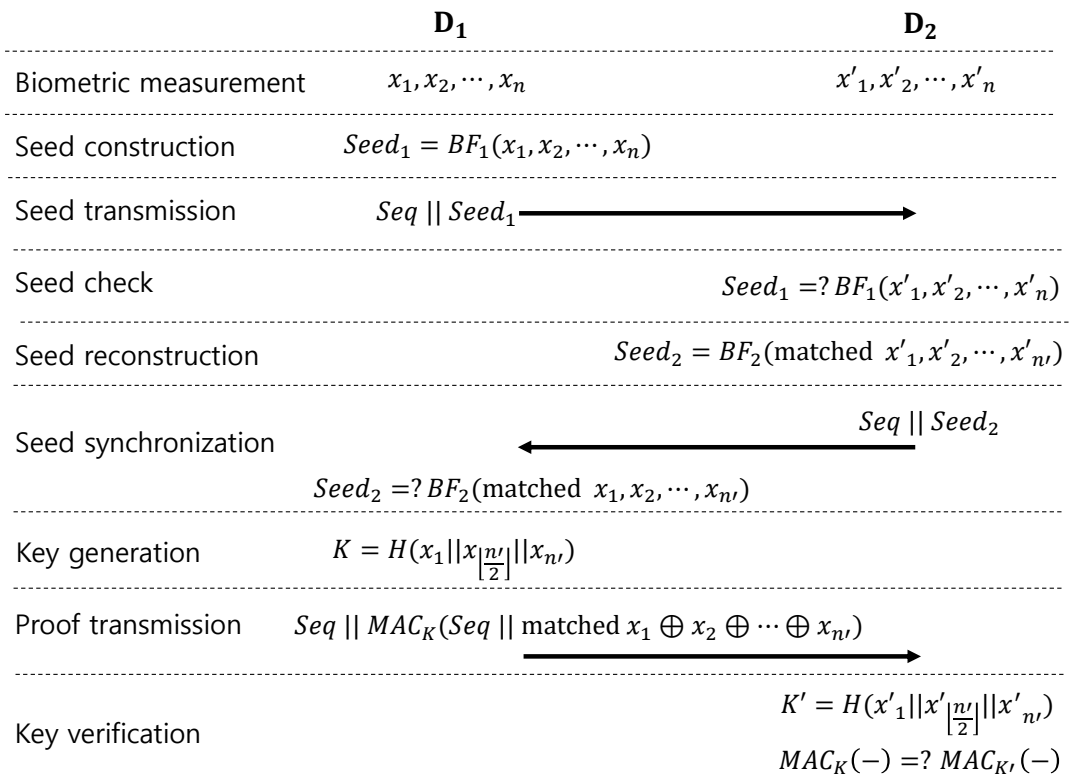

Figure 3: Proposed biometric key agreement between two biometric sensor devices D_1 and D_2

in order to look up member y in the group, we carry out k hash computations of the member and then we check whether the corresponding bits are ones. Since the bits contains zero at $h_2(y_1)$, the member y_1 cannot be a member of the group. In case of member y_2, the member is in the group or the filter may generate a false-positive error. In most applications, however, a false-positive error is sufficiently small to be acceptable [11]. To avoid trivialities, we decide $m \gg kn$ in our scheme. In Section 3.2, we prove that the false-positive errors of our scheme are negligibly small.

3 Proposed Scheme

3.1 Biometric Key Agreement

The entire process of the proposed scheme is described in Fig. 3. The proposed scheme consists of the following nine steps:

Biometric measurement. Two biometric sensor devices D_1 and D_2 measure physiological signals while generating physiological-signal-based features every a given period. We define n feature values of both devices as $\{x_1, x_2, \cdots, x_n\}$ and $\{x'_1, x'_2, \cdots, x'_n\}$, respectively. Ideally, two biometrics should be identical only if they were measured at the same time; however, mostly, the measurement result is not complete. This problem would be alleviated by using existing error correction functions (ECFs) [13, 14]. We assume that the errors of feature values are already corrected up to the acceptable number of bits by using the existing ECFs.

Seed construction. For an identical session key generation between two devices D_1 and D_2, the both devices should generate the same seed, which will be used as input of session key generation function. In this step, device D_1 constructs its own seed, $Seed_1$, using bloom filter $BF_1(\cdot)$ and n number of biometrics $x_1, x_2, \cdots, x_n$ which it measured.

Seed transmission. The device D_1 transmits the seed $Seed_1$ to D_2 along with assigned sequence Seq.

Seed check. The device D_2 checks whether or not each biometric of $x'_1, x'_2, \cdots, x'_n$ is in $Seed_1$ through member checking, as introduced in Section 2.2.

Seed reconstruction. Here, "matched $x'_1, x'_2, \cdots, x'_{n'}$" stands for certain biometrics which pass the above seed check; $n' \leq n$. In other words, it means that the matched biometrics are common biometrics between devices D_1 and D_2. Device D_2 produces seed $Seed_2$ using the matched biometrics and another bloom filter $BF_2(\cdot)$. If this

step employs the same bloom filter BF_1 as the seed construction step, an adversary can derive some information for a session key via correlation analysis of two seeds $Seed_1$ and $Seed_2$.

Seed synchronization. The device D_2 sends the seed $Seed_2$ to D_1 along with sequence Seq received from device D_1. Through member checking, device D_2 can confirm which biometrics among its own biometrics are matched to biometrics generated by device D_2.

Key generation. If the matched biometrics can make the same seed $Seed_2$, device D_2 makes session key K using a given key derivation method, here, one-way hash function H with the input of $x_1 \parallel x_{\lfloor \frac{x}{2} \rfloor} \parallel x_{n'}$; $x_{\lfloor \frac{x}{2} \rfloor}$ is a median value. Otherwise, the key generation step is failed and then the key agreement process begins from the first step again. The key derivation method can be substituted as any valid key derivation method.

Proof transmission. For key agreement between two devices, device D_1 computes proof $MAC_K($ matched $x_1 \oplus x_2 \oplus \cdots \oplus x_{n'})$ and then it transmits the proof to device D_2 with its sequence. $MAC_K(\cdot)$ is a message authentication code using session key K for a given message and $\oplus$ is a XOR operator. The matched $x_1 \oplus x_2 \oplus \cdots \oplus x_{n'}$ means XOR operations among all matched biometrics.

Key verification. Using the same key derivation method employed by device D_1 in the key generation step, device D_2 can create the same session key K', i.e., $K' = K$. After that, device D_2 calculates its message authentication code with the inputs corresponding to the previous step. Then device D_2 checks whether the calculated MAC $MAC_{K'}($ matched $x'_1 \oplus x'_2 \oplus \cdots, x'_{n'})$ is equal to the received MAC $MAC_K($ matched $x_1 \oplus x_2 \oplus \cdots \oplus x_{n'})$. Finally, if equal, two devices D_1 and D_2 generate the same session key. Otherwise, the key agreement process is failed and then new key agreement process will begin using new n biometrics.

3.2 False-positive Errors

We now analyze the false-positive errors of the proposed scheme. We assume that a hash function chooses each bit position with the same probability. Let m, k, and n denote the number of bits forming the bloom filter, the number of hash functions, and the number of biometrics used as the input of the bloom filter, respectively. For the member checking of a biometric for a given seed, if all of the k bit positions in the bloom filter are set to one, the bloom filter perceives that the biometric is a member of the seed. As shown in [15], the probability of this happening when the biometric does not belong to the seed is followed by

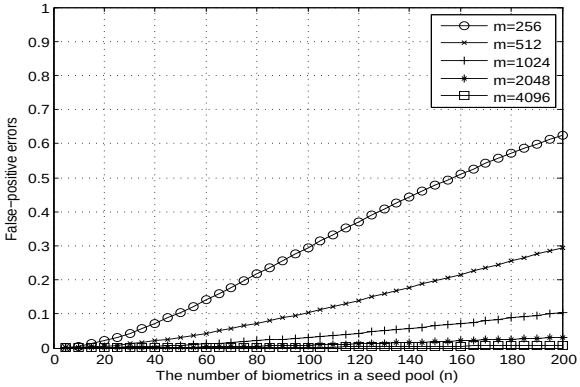

Figure 4: False-positive errors ($k = 2$).

$$\left(1 - \left(1 - \frac{1}{m}\right)^{kn}\right)^k. \quad (1)$$

Fig. 4 illustrates the false-positive probability of the proposed scheme according to the size (from 256 to 4,096 bits) of the bloom filter size having two hash functions. If we limit the size of the bloom filter and the maximum number of biometrics used for a seed construction as $m = 4,096$ and $n = 100$ ($m \gg k \times n$), respectively, the false-positive probability will be negligibly tiny.

4 Conclusion

In this paper, we introduce new biometric-based key agreement scheme between devices in body sensor networks. Unlike existing schemes, the proposed scheme needs neither pre-deployed secret information embedded in devices nor public cryptography algorithms requiring high computational costs.

In near future, we will study error correction algorithm for two biometrics measured from the same body simultaneously. Furthermore, we will develop the entire process from the biometric measurement to the biometric key agreement.

Acknowledgements: This work was supported by the ICT R&D program of MSIP/IITP [B0117-16-1002, Feasibility Study of Blue IT based on Human Body Research].

References:

[1] A. Greenberg, *OPM Now Admits 5.6m Feds' Fingerprints Were Stolen By Hackers,* https://www.wired.com/2015/09/opm-now-admits-5-6m-feds-fingerprints-stolen-hackers/, 2015.

[2] L. Arsene, *Hacking Vulnerable Medical Equipment Puts Millions at Risk,* http://www.informationweek.com/partner-perspectives/bitdefender/hacking-vulnerable-medical-equipment-puts-millions-at-risk/a/d-id/1319873, 2015.

[3] R. Console, *Hacking Your Life: A Worst-Case Scenario for Implanted Medical Devices,* http://www.myinjuryattorney.com/law-blog/hacking-your-life-a-worst-case-scenario-for-implanted-medical-devices/, 2013.

[4] M. Rostami, A. Juels, and F. Koushanfar, *Heart-to-Heart (H2H): Authentication for Implanted Medical Devices,* ACM CCS'13, 2013, pp. 1099-1112.

[5] E. K. Zaghouani, A. Jemai, A. Benzina, and R. Attia, *ELPA: A new key agreement scheme based on linear prediction of ECG features for WBAN,* 23rd European Signal Processing Conference (EUSIPCO), 2015.

[6] C. Hu, X. Cheng, F. Zhang, D. Wu, X. Liao, and D. Chen, *OPFKA: Secure and efficient Ordered-Physiological-Feature-based key agreement for wireless Body Area Networks,* IEEE Infocom, 2013, pp. 2274-2282.

[7] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, *PSKA: Usable and Secure Key Agreement Scheme for Body Area Networks,* IEEE Trans. Information Technology in Biomedicine, 14(1), 2010, pp. 60-68.

[8] G. H. Zhang, Carmen C. Y. Poon, and Y. T. Zhang, *A Biometrics Based Security Solution for Encryption and Authentication in Tele-Healthcare Systems,* 2nd Int. Symp. Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2009.

[9] 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,* Int. Conf. Parallel Processing Workshops, 2003.

[10] M. Roeschlin, I. Sluganovic, I. Martinovic, G. Tsudik, K. B. Rasmussen, *Generating Secret Keys from Biometric Body Impedance Measurement,* ACM on Workshop on Privacy in the Electronic Society ACM on Workshop on Privacy in the Electronic Society (WPES), 2016, pp. 59-69.

[11] A. Broder, M. Mitzenmacher,and A. Broder, *Network Applications of Bloom Filters: A Survey,* Internet Mathematics, vol. 1, 2002, pp. 636-646.

[12] 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, 2006, pp. 73-81.

[13] A. Juel and M. Wattenberg, *A fuzzy commitment scheme,* 6th ACM Conference on Computer and Communication security, 1999, pp. 28-36.

[14] I. S. Reed and X. Chen, *Error-Control for Data Networks,* Kluwer Academic Publishers, 1999.

[15] S. Tarkoma, C. E. Rothenberg, and E. Lagerspetz, *Theory and Practice of Bloom Filters for Distributed Systems,* IEEE Communications Surveys&Tutorials, 14(1), 2012, pp. 131-155.