Deriving cryptographic keys from physiological signals

Duygu Karaoğlan Altop, Albert Levi, Volkan Tuzcu

PII:	S1574-1192(16)30130-4
DOI:	http://dx.doi.org/10.1016/j.pmcj.2016.08.004
Reference:	PMCJ 738
To appear in:	*Pervasive and Mobile Computing*
Received date:	6 February 2016
Revised date:	28 July 2016
Accepted date:	14 August 2016

Please cite this article as: D.K. Altop, A. Levi, V. Tuzcu, Deriving cryptographic keys from physiological signals, *Pervasive and Mobile Computing* (2016), http://dx.doi.org/10.1016/j.pmcj.2016.08.004

Deriving Cryptographic Keys from Physiological Signals[☆,☆☆]

Duygu Karaoğlan Altop[a,*], Albert Levi[a], Volkan Tuzcu[b]

[a] *Faculty of Engineering and Natural Sciences, Sabancı University, Istanbul, TURKEY*
[b] *Department of Pediatric Cardiology, İstanbul Medipol University, Istanbul, TURKEY*

Abstract

Biosensors aim at providing pervasive healthcare by collecting and communicating highly sensitive medical information. Due to their extreme limitations, lightweight and secure key management infrastructures are required. For this reason, biosensors use physiological parameters that are generated from different vital signals (i.e., electrocardiogram, photoplethysmogram, blood pressure) to protect the exchanged private health information. In this paper, we define two novel physiological parameter generation techniques and analyze both the performance and the quality of the outcomes. Our results show that we generate good candidates of physiological parameters that can be used as cryptographic keys to secure the communication among the biosensors.

Keywords: Cryptographic Key Generation; Body Area Networks; Physiological Signals; Bio-cryptography

1. Introduction

Healthcare concerns with the maintenance or restoration of an individual's health by preventing or treating well-being through medical services. With the use of pervasive computing, healthcare systems can be constituted so as to enable remote, continuous and real-time health monitoring. While using pervasive healthcare, physical presence of the health professionals are required only during emergencies; meaning that there is no restriction on the time and space of the patient monitoring process. Body Area Networks (BANs), whose infrastructure is depicted in Figure 1, are the most important building block of pervasive healthcare [2–4]. They provide effective, efficient and accurate monitoring of

[☆] This work was partially supported by the Scientific and Technological Research Council of Turkey (TÜBİTAK) under grant 114E557 and part of this work was presented in PervasiveHealth 2015 [1].

[☆☆] Duygu Karaoğlan Altop was supported by TÜBİTAK BİDEB 2211-C.

[*] Corresponding author

Email addresses: duyguk@sabanciuniv.edu (Duygu Karaoğlan Altop), levi@sabanciuniv.edu (Albert Levi), vtuzcu@gmail.com (Volkan Tuzcu)