

Accepted Manuscript

A Secure Biometrics-Based Authentication Key Exchange Protocol for Multi-Server TMIS using ECC

Mingping Qi , Jianhua Chen , Yitao Chen

PII: S0169-2607(18)30526-1
DOI: [10.1016/j.cmpb.2018.07.008](https://doi.org/10.1016/j.cmpb.2018.07.008)
Reference: COMM 4754



To appear in: *Computer Methods and Programs in Biomedicine*

Received date: 16 April 2018
Revised date: 15 June 2018
Accepted date: 16 July 2018

Please cite this article as: Mingping Qi , Jianhua Chen , Yitao Chen , A Secure Biometrics-Based Authentication Key Exchange Protocol for Multi-Server TMIS using ECC, *Computer Methods and Programs in Biomedicine* (2018), doi: [10.1016/j.cmpb.2018.07.008](https://doi.org/10.1016/j.cmpb.2018.07.008)

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

Highlights

- A secure biometrics-based authentication key exchange protocol for multi-server TMIS using elliptic curve cryptography is proposed.
- Unlike some relevant existing schemes, the registration center of the proposed scheme needn't to share system private key with distributed servers.
- The security analysis by BAN logic and heuristic cryptanalysis shows the proposed scheme is a secure authentication scheme for multi-server TMIS.

ACCEPTED MANUSCRIPT

Download English Version:

<https://daneshyari.com/en/article/6890692>

Download Persian Version:

<https://daneshyari.com/article/6890692>

[Daneshyari.com](https://daneshyari.com)