Reza Ghasemi

Bu-ali Sina University
Science Department
Hamedan, Iran
r.ghasemi@basu.ac.ir

Work

Assistant Professor at Bu-ali Sina University, Hamedan, Iran.

Interests

Cryptography protocols, Data Outsourcing, Blockchain
Cloud Computing, Lattice Based Cryptography.

Education

Iran University of Science and Technology
Ph.D., Mathematics, 2012 - 2016, *GPA 18.71*.
Thesis: Learning with error and its applications in cryptography.

Sharif University of Science and Technology
M.Sc., Cryptography, 2010 - 2012, *GPA 16.73*.
Dissertation: Dynamic Multi-Stage Multi-Secret Sharing Scheme

Bu-ali Sina University
B.Sc., 2006 - 2010, *GPA 18.17*.

Visit

Computer Science Department, University of Manitoba, Manitoba, Canada
6 months
Project: Outsourcing genome data to a database.

Computer Science Department, Koc University, Istanbul, Turkey
1 month
Project: Biometric authentication scheme.

Teaching

Faculty of Science, Bu-ali Sina University
Algorithm and Computation.
Introduction to Cryptography.
Combinatorics.
Differential Equations.
Number Theory
Olympiad preparation
Calculus

Mathematics Department, Iran University of Science and Technology
Complex Variables.

Students

Somaye Bahrami (M.Sc.)
Thesis: Searchable Data Outsourcing Based on Secret Sharing Schemes

Mohsen Yari Mojahed (M.Sc.)
Thesis: Secure similar patients query on outsourced genomic databases

Reza Mamivand (M.Sc.)
Thesis: Reducing required storage space in blockchain systems using multisecret sharing schemes

Roonak Mahmodian (M.Sc.)
Thesis: A decentralized storage scheme based on Ethereum blockchain smart contracts for storing and querying pharmacogenomics data

Awards

(All certificates are received)

2019
Best University Lecturer in Mathematics

2016
-Selected solution in 2016 IDASH Genome Privacy and Security Competition, Task 1:Practical Protection of Genomic Data Sharing through Beacon Services.

2010
-Ranked first, among nearly 12,000 participants in the National University Entrance Exam for M.Sc. in Mathematics,

-Bronze Medal, 34th Iranian National Mathematics Competition for University Students

-Ranked 12th, International Mathematics Olympiad, Iran

2006 - 2010
-Ranked first in B.Sc between 32 students

Papers

Resolving a common vulnerability in secret sharing scheme–based data outsourcing schemes.
-Concurrency and Computation: Practice and Experience.

Private and Efficient Query Processing on Outsourced Genomic Databases.
-IEEE Journal of Biomedical and Health Informatics.

Aftermath of Bustamante Attack on Genomic Beacon Service.
-BMC Medical Genomic.

Efficient multistage secret sharing scheme using bilinear map.
-IET information theory.

A Lightweight Public Verifiable Multi Secret Sharing Scheme Using Short Integer Solution.
-Wireless Personal Communications.

Efficient multisecret sharing scheme using new proposed computational security model.
-International Journal of Communication Systems.

Seminar	**How Does Bitcoin Work?(At Bu-Ali Sina University)**
Referee	**Recent Patents on Computer Science** **Security and Communication Networks** **48th Annual Iranian Mathematics Conference**
Programming	**Python** **Js** **Java** **Solidity**
Current Projects	**Reducing ledger size in blockchains with the help of secret sharing** **Sharing pharmacological information using Ethereum smart contract** **Query over outsourced databases based on secret sharing**
Languages	**Farsi (Mother tongue)** **English (Ielts Overall 7)** **Turkish (Elementary)**
Operational	**Supervisor of Bu-Ali Sina University team in 43rd Iranian National Mathematics Competition for University Students**

References

Prof. Noman Mohammed
University of Manitoba
Department of Computer Science
noman@cs.umanitoba.ca
cs.umanitoba.ca/∼ noman

Prof. Taraneh Eghlidos
Sharif University of Technology
Electronics Research Institute
teghlidos@sharif.edu
sharif.edu/∼ teghlidos

Dr. Yahya Hassanzadeh
Senior Distributed System Engineer
(Ph.D.) Dapper Labs
yahya@dapperlabs.com
sites.google.com/view/yhassanzadeh