Mohammad Etemad, PhD

Curriculum Vitae
September 01, 2017

University of Virginia, Charlottesville, VA
Phone: (+1) 434 906 6088
Email: etemad@virginia.edu, m.etemad@gmail.com
Homepage: http://www.metemad.info/

Research Interests

- Applied Cryptography
- Searchable Encryption
- Access Control in the Cloud
- Provable Secure Cloud Storage
- Secure Outsourced Database
- Security in Mobile and Social Networks

Education

- University of Virginia, VA, USA (2015 -)
  Postdoctoral Research Associate, Advisor: David Evans
- Koç University, Istanbul, Turkey, 2015
  Ph.D. in Computer Science, Advisor: Alptekin Küpçü
  Thesis: Reliable Cloud Storage using Hierarchical Authenticated Data Structures
- Sharif University of Technology, Tehran, Iran, 2008
  M.Sc. in Software Engineering, Advisor: Rasool Jalili
  Thesis: Security Vulnerabilities of the GSM Network
- Amirkabir University of Technology, Tehran, Iran, 2002
  B.Sc. in Software Engineering, Advisor: Mohammad Reza Meybodi
  Thesis: Design of a Financial Transaction Log Analyzer using Expert Systems

Publications

- **Etemad, M.**, Küpçü, A., Papamanthou, C., Evans, D., **Efficient Dynamic Searchable Encryption with Forward Privacy**, *to appear in PETS 2018*.
- **Etemad, M.**, Barto, F., Küpçü, A., Preneel, B., **Efficient and Secure Friend-finding in Mobile Social Networks**, *SEMS 2017*, France, 2017.
- **Etemad, M.**, Küpçü, A., **Generic Efficient Dynamic Proofs of Retrievability**, *CCSW'16*, Austria, 2016.
- **Etemad, M.**, Küpçü, A., **Efficient Key Authentication Service for Secure End-to-end Communications**, ProvSec 2015, Japan, 2015.
- **Etemad, M.**, Küpçü, A., **Database Outsourcing with Hierarchical Authenticated Data Structures**, ICISC 2013, South Korea, 2013.
- **Etemad, M.**, Küpçü, A., **Transparent, Distributed, and Replicated Dynamic Provable Data Possession**, ACNS 2013, Canada, 2013.
- **Etemad, M.**, Anvari, S., **A Semi-Linear Relation between Inputs and Outputs of DES S-Boxes**, International Journal of Computer Applications, vol. 56, issue 9, pp. 39-42, 2012.
- Salehpour, A., **Etemad, M**., Mokhtari Nazarlu, **Intelligent Guard: A Novel Approach toward Software Protection**, Springer, Informatics Eng. and Info. Science, PP. 449-460, 2011.
- **Etemad, M.**, **A New and Efficient Authentication Protocol for GSM Networks**, CSICC09, Tehran Iran, 2009 (In Farsi).

- **Under review:**

- **Etemad, M.**, Mahmoody, M., Evans, D., **Optimizing Trees for Searchable Encryption**, *submitted to PETS 2018*.
- **Etemad, M.**, Küpçü, A., **A Generic Dynamic Provable Data Possession Model**, *submitted to IEEE ToCC*.

- **Etemad, M.**, Küpçü, A., **Verifiable Database Outsourcing Supporting Join**, *submitted to JNCA*.
- **Etemad, M.**, Küpçü, A., **Verifiable Dynamic Symmetric Searchable Encryption Supporting Boolean Search**, *submitted to Turkish Journal of Electrical Engineering and Computer Sciences.*

Patents

- Efficient dynamic proofs of retrievability (granted).

Work Experiences

- **Project Manager,** Tosan Co (http://www.tosan.com/en/default.aspx), Tehran, 2005-2007 (TOSAN is the first and largest market-leading provider of banking software solutions to retail, corporate, private, and microfinance banks in Iran.):
  - Leading and administrating a software development team consisting of 7 programmers.
    - The LC subsystem of a whole banking system was designed and developed.
    - An "accounting documents management" subsystem was developed.
- **Programmer,** Tosan Co (http://www.tosan.com/en/default.aspx), Tehran, 2002-2005:
  - The Wage and Welfare subsystem of a whole banking system was implemented.
  - A subsystem for generating and interpreting SWIFT messages (part of the whole banking system) was designed and developed.
- **Tester,** AmirKabir University of Technology, Tehran, 1999-2000:
  - Testing the firewall "Hadid" developed at the Sharif University.

Talks

- **Access Control in the Cloud**, University of Virginia, Charlottesville, VA, 2016.
- **Efficient Key Authentication Service for Secure End-to-end Communications**, ProvSec 2015, Japan.
- **Secure Cloud Storage Services using Hierarchical Authenticated Data Structures,** KU Leuven, Belgium, 2015.
- **Oblivious RAM: Progress and Applications**, Koç University, Istanbul, Turkey, 2014.
- **Database Outsourcing with Hierarchical Authenticated Data Structures**, ICISC 2013, South Korea.
- **Transparent, Distributed, and Replicated Dynamic Provable Data Possession**, ACNS 2013, Canada

Teaching Experiences

- University College of NabiAkram (UCNA), Tabriz, Iran, Fall 2007 - Spring 2011
  - Courses taught: Introduction to Algorithm Design, Software Design, Operating Systems, Theory of Formal Languages and Automata.
  - Directed and supervised 15 undergraduate student theses.
- University of Tabriz, Tabriz, Iran, Spring 2011
  - Courses taught: Foundations of IT.

Honors and Awards

- $3000 research award, funded by Koç University.
- Koç University full scholarship for PhD program.
- 5th rank in the Iranian universities M.Sc. program entrance exam.
- 488th rank among ~500,000 participants in the Iranian universities entrance exam (B.Sc.).

Languages

- Azerbaijani, Persian: Native
- Turkish, English: Fluent