Mohammad Shahriar Rahman

Contact Information

JAIST Dormitory 1-509,
1-8 Asahidai, Nomi
Ishikawa, Japan 923-1211
http://grampus.jaist.ac.jp/student/mohammad.htm

Mobile: +81-80-3044-9448
Fax: +81-761-51-1405
mohammad@jaist.ac.jp

Objective

Placement in a faculty position that allows for advanced research in the field of Applied Cryptography and Information Security.

Research Interests

Applied Cryptography, Privacy-preserving Data Mining, Privacy in Resource Constrained Devices, Game Theory (Rational Cryptography)

Professional Experience

National Institute of Information and Communications Technology (NICT), Tokyo, Japan

R&D Intern at Security Architecture Lab **August 2011 to October 2011**

- Studied SHAREMIND: A Platform for Privacy Preserving Data Mining.

Education

Ph.D., **Japan Advanced Institute of Science and Technology (JAIST)**, Ishikawa, Japan,
Information Science, March 2012 (expected)

- Thesis Topic: *Constructing Privacy Preserving Cryptographic Protocols*
- Adviser: Professor Atsuko Miyaji, JAIST
- Sub-theme Adviser: Associate Professor Masakazu Soshi, Hiroshima City University
- Area of Study: Information Security

M.Sc., **Japan Advanced Institute of Science and Technology (JAIST)**, Ishikawa, Japan,
Information Science, March 2009

- Thesis Topic: *On Security and Privacy Enhanced Authentication on RFID*
- Adviser: Professor Atsuko Miyaji, JAIST
- Sub-theme Adviser: Professor Tadashi Matsumoto, JAIST
- Area of Study: Information Security

B.Sc. (Hons), **University of Dhaka**, Dhaka, Bangladesh,
Computer Science and Engineering, July 2006

Refereed Journal Publications

"KIMAP: Key-Insulated Mutual Authentication Protocol for RFID"- *International Journal of Automated Identification Technology, (IJAIT)*. With Atsuko Miyaji. To Appear.

"Dynamic Attribute based Signcryption without Random Oracles"- *International Journal of Applied Cryptography (IJACT)*. With Keita Emura and Atsuko Miyaji. To Appear.

"A Low Cost and Secure RFID Authentication Scheme" - *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*. With Atsuko Miyaji and Masakazu Soshi. Vol 2, No 3, pp. 4-25, 2011.

Submitted Journal Publications

"Privacy-preserving Two-party Rational Set Intersection Protocol". With Atsuko Miyaji. Submitted.

"Privacy-preserving Dot-Product Protocols in Malicious and Covert Adversarial Models". With Keita Emura and Atsuko Miyaji. Submitted.

"Ideal Secret Sharing Schemes with Share Selectability and its Application to Distributed Systems with General Access Structures". Keita Emura, Atsuko Miyaji, Akito Nomura, and Masakazu Soshi. Submitted.

Conference Publications

"Ideal Secret Sharing Schemes with Share Selectability"- *The 13th International Conference on Information and Communications Security, ICICS 2011*, Lecture Notes in Computer Science, 7043 (2011), Springer-Verlag. With Keita Emura, Atsuko Miyaji, Akito Nomura, and Masakazu Soshi. November 23 - 26, Beijing, China.

"Privacy-Preserving Data Mining: A Game-theoretic Approach"- *The 25th IFIP WG 11.3 Conference on Data and Applications Security and Privacy, DBSec 2011*, Lecture Notes in Computer Science, 6818 (2011), Springer-Verlag. With Atsuko Miyaji. July 11 - 13, Virginia, USA.

"Toward Dynamic Attribute-based Signcryption"- *The 16th Australasian Conference on Information Security and Privacy, ACISP 2011*, Lecture Notes in Computer Science, 6812 (2011), Springer-Verlag. With Keita Emura and Atsuko Miyaji. July 11 - 13, Melbourne, Australia.

"Efficient Privacy-Preserving Data Mining in Malicious Model"- *The 6th International Conference on Advanced Data Mining and Applications, ADMA 2010*, Lecture Notes in Computer Science, 6440 (2010), Springer-Verlag. With Keita Emura and Atsuko Miyaji. November 19 - 21, Chongqing, China. **(Best Paper Award)**

"Privacy-Preserving Data Mining in Presence of Covert Adversaries"- *The 6th International Conference on Advanced Data Mining and Applications, ADMA 2010*, Lecture Notes in Computer Science, 6440 (2010), Springer-Verlag. With Atsuko Miyaji. November 19 - 21, Chongqing, China.

"Hidden Credential Retrieval Without Random Oracles"- *The 11th International Workshop on Information Security Applications, WISA 2010*, Lecture Notes in Computer Science, 6513 (2010), Springer-Verlag. With Atsuko Miyaji and Masakazu Soshi. August 24 - 26, Jeju Island, South Korea.

"APRAP: Another Privacy Preserving RFID Authentication Protocol"- *The 6th workshop on Secure Network Protocols, NPSec 2010*, IEEE. With Atsuko Miyaji. October 5, Kyoto, Japan.

"A Secure RFID Authentication protocol with Low Communication Cost"- *The 3rd International Workshop on Intelligent, Mobile and Internet Services in Ubiquitous Computing, IMIS 2009*, IEEE. With Atsuko Miyaji and Masakazu Soshi. March 16 - 19, Fukuoka, Japan.

Other Publications

"Privacy-Preserving Set Operations in the Presence of Rational Parties- Information Security, IEICE Japan Technical Report, ISEC 2011-11.

"Authenticating RFID Tags using Insulated Keys"- Information and Communication System Security, IEICE Japan Technical Report, ICSS 2009-11.

Mohammad Shahriar Rahman *On Security and Privacy Enhanced Authentication on RFID*. Master's thesis, JAIST, Ishikawa, Japan, 2009.

"An RFID Authentication Protocol Suitable for Batch-mode Authentication"- Computer Security Symposium, CSS 2008.

"A Study on Turbo Code Design, Performance Analysis and Decoding Techniques- Master's Sub-theme Research Report, submitted to Multimedia Systems Lab, JAIST 2008.

"Elliptic Curve Addition, Doubling and Scalar Multiplication in Jacobian coordinate system- Summer Study Technical Report, submitted to System Control & Management Lab, JAIST 2007.

As is standard in the theoretical computer science community, author names for papers published in journals or conference proceedings are listed in alphabetical order.

Referee Service

- *IEICE Transactions on Information and Systems*
- *International Journal of Radio Frequency Identification Technology and Applications*
- *International Journal of Communication Networks and Information Security*
- *The 2011 Workshop on RFID Security- RFIDSec'11 Asia*
- *The 14th Information Security Conference- ISC 2011*
- *The 10th International Conference on Cryptology and Network Security- CANS 2011*
- *The 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications- TRUSTCom 2011*
- *The 14th Australasian Conference on Information Security and Privacy- ACISP 2009*

Conference Service (Member of the Local Organizing Committee:)

The 29th Symposium on Cryptography and Information Security- SCIS 2012, Kanazawa, Japan, January 30 - February 2, 2012

The 4th International Conference on Pairing-Based Cryptography- Pairing 2010, Yamanaka Hot Spring, Japan, December 13 -15, 2010.

The 8th International Conference on Cryptology And Network Security- CANS 2009, Kanazawa, Japan, December 12 -14, 2009.

Awards

- Monbukagakusho Scholarship (Ministry of Education, Culture, Sports, Science and Technology- MEXT, Govt. of Japan) since October 2006 till date.
- Partial research grant (Grant No.: 2011.1.2.072, International Information Science Foundation, Japan) for the work published in DBSec 2011.
- Partial research grant (Grant-in-Aid for Scientific Research (C): 20500075, MEXT) for the work published in WISA 2010.
- **Best Paper Award** at The 6th International Conference on Advanced Data Mining and Applications (ADMA), 2010.
- **Excellent Student Award** from The Institute of Electronics, Information and Communication Engineers (IEICE), 2009.
- Dhaka Education-Board Merit Scholarship in Bangladesh for academic excellences in 'Higher Secondary School Certificate (H.S.C.) Examinations (equivalent to High School Graduation), 1999.
- Dhaka Education-Board Merit Scholarship in Bangladesh for academic excellences in 'Secondary School Certificate (S.S.C.) Examinations (equivalent to 10th grade; placed 15th in the merit list in Dhaka board), 1997.

Teaching Experience

Japan Advanced Institute of Science and Technology, Ishikawa, Japan

Teaching Assistant **April 2009 to December 2011**

- Teaching Assistant for I 216: Computational Complexity and Discrete Mathematics
  - Spring 2009, Autumn 2009, Spring 2010, Autumn 2010, Spring 2011, Autumn 2011
  - Assisted the instructor during lecture.
  - Provided in-class support to graduate students.
  - Graded weekly assignments.
  - Responsible for 1.5 hour office hour per week to discuss with the students on various problems of I 216 and giving solutions of the weekly assignments.

Teaching Assistant **April 2008 to September 2011**

- Teaching Assistant for I 461S: Current Topics in Information Security
  - Assisted the instructor during lecture.
  - Provided in-class support to the students of Kyoto University, Osaka University, NAIST and JAIST who enrolled for this course.
  - Responsible for supervision of 1.5 hour programming laboratory where students solve various cryptographic problems and implement cryptographic protocols.
  - Graded weekly assignments on security programming and cryptographic problems.

Teaching Assistant **August 2008 to August 2010**

- Teaching Assistant for 3 day long Summer School on Information Security at JAIST
  - Assisted the instructor during lecture.
  - Provided in-class support to the students.
  - Responsible for supervision of 7 hour security programming laboratory.

Teaching Assistant **July 2010**

- Teaching Assistant for 3 day intensive course on Information Security at Kyoto University
  - Assisted the instructor during lecture.
  - Provided in-class support to the students.
  - Responsible for 8 hour long instruction for the students on various assignments and their solutions.

Research Experience

Japan Advanced Institute of Science and Technology, Ishikawa, Japan

Research Assistant **April 2009 to Present**

- Participated in various projects on privacy preserving protocols.
- Designed and verified cryptographic protocols.
- Prepared and presented papers on the research results.

Membership

The International Association for Cryptologic Research (IACR), Student Member, 2011–present

Institute for Electrical and Electronics Engineers (IEEE) Computer Society, Student Member, 2009–present

Institute of Electronics, Information and Communication Engineers (IEICE), Student Member, 2009–present

Presentation and Talks

"Privacy-Preserving Set Operations in the Presence of Rational Parties- Information Security IEICE, ISEC 2011, at Osaka Electro-Communication University, Japan. (in November, 2011)

"Efficient Privacy-Preserving Data Mining in Malicious Model" – The 6th International Conference on Advanced Data Mining and Applications, ADMA 2010, at Wanyou Conifer Hotel, Chongqing, China. (in November 2010)

"Privacy-Preserving Data Mining in Presence of Covert Adversaries" – The 6th International Conference on Advanced Data Mining and Applications, ADMA 2010, at Wanyou Conifer Hotel, Chongqing, China. (in November 2010)

"Hidden Credential Retrieval Without Random Oracles" – The 11th International Workshop on Information Security Applications, WISA 2010, at Ramada Plaza, Jeju Island, South Korea. (in August 2010)

"Authenticating RFID Tags using Insulated Keys"– Information and Communication System Security IEICE, ICSS 2009, at Miyazaki University, Miyazaki, Japan. (in November 2009)

"A Secure RFID Authentication protocol with Low Communication Cost"– The 3rd International Workshop on Intelligent, Mobile and Internet Services in Ubiquitous Computing, IMIS 2009, at Fukuoka Institute of Technology, Fukuoka, Japan. (in March 2009)

"An RFID Authentication Protocol Suitable for Batch-mode Authentication" – Computer Security Symposium, CSS 2008, at Convention Center of Naha, Okinawa, Japan. (in October 2008)

Some Graduate Courses Discrete Mathematics, Analysis for Information Science (Digital Signal Processing), Computer Networks, Mathematical Logic, Human Information Processing, Speech Signal Processing, Information Systems (Next Generation Internet Technology), Information Processing Theory, Operating Systems, Scientific Discussions and Critical Thinking.

References Available upon Request.