Curriculum Vitae of Mridul Nandi 2012

Name

MRIDUL NANDI

Present institutional address with telephone, fax and e-mail

203 B. T. Road, Applied Statistics Unit, Indian Statistical Institute, Kolkata
Phone: +91-33-25752001
Fax: +91-33-25776925
email: director@isical.ac.in
web site: www.isical.ac.in

Address for correspondence with telephone and e-mail

18, Jugipara lane, Rathtala, Barasat-700124. W.B., India
Telephone: +91-9681961246,
email: mridul.nandi@gmail.com

Date of Birth

21st June 1977.

Academic qualifications

1. **Ph.D.** in Computer Science **2002 - 2005**
Indian Statistical Institute, Kolkata.
Thesis Title: Designs of Iteration on Hash Functions and its Cryptanalysis.
Supervisor: Prof. Bimal Roy, Director of Indian Statistical Institute.

2. **M.Stat.** (Master Degree in Statistics) **1999 - 2001**
Indian Statistical Institute
Specialization : *Mathematical Statistical Probability* or MSP.
First division with distinction

3. **B.Stat.** (Bachelor Degree in Statistics) **1996 - 1999**
Indian Statistical Institute
First division with distinction

Details of Employment and Nature of Duties

1. **Jun 2011 - till now**: Assistant Professor in Applied Statistics Unit, Indian Statistical India, Kolkata.
2. **Oct 2010 - May 2011**: Associate Professor in C R Rao AIMSCS, Hyderabad, India performing leading research in different aspects of Cryptography.
3. **Oct 2009 - Aug 2010**: Senior Research Associate in The George Washington University, analyzing, modifying and implementing cryptographic voting protocols.
4. **May 2008 - Oct 2009**: Visiting Researcher in the NIST for running the SHA-3 Hash Competition Project in **NIST**. Dr. Mridul Nandi is a member of the committee that evaluates all submitted candidates to choose eligible candidates among them to proceed to the next round. This project is still on going and supposed to progress until 2012.

5. **Mar 2008 - May 2008**: Visiting Scientist at **Indian Statistical Institute**, Kolkata.
6. **Jun 2007 - Mar 2008**: Assistant Professor in **CINVESTAV, IPN**, Mexico City, Mexico, teaching graduate courses and performing cryptographic research.
7. **Apr 2007 - May 2007**: Visiting Scientist at **Indian Statistical Institute**, Kolkata for performing leading research in the different aspects of Cryptography.
8. **Apr 2006 - Mar 2007**: Post-doctoral researcher at the **University of Waterloo**, Canada, under the supervision of Prof. Douglas R. Stinson, performing research on hash function as a continuation of Dr Nandi's thesis work.
9. **Dec 2005 - Mar 2006**: Visiting Scientist at **Institut national de recherche en informatique et en automatique** (INRIA), Rocquencourt, France, performing research on hash function as a continuation of Dr Nandi's thesis work.
10. **Feb 2002 - Jun 2002**: **Software Analyst** in a multinational company **Cognizant Technological Solution** (CTS), Kolkata.
11. **Aug 2001 - Jan 2002**: **Stock Market Analyst** in **East India Security**, National Stock Exchange, Kolkata for analyzing and predicting stock price by using some statistical methods.

Visiting Scientist at the following places

Indian Statistical Institute, Kolkata.	Mar 2008 - May 2008.
Indian Statistical Institute, Kolkata.	Apr 2007 - May 2007.
INRIA, Rocquencourt, France,	Dec 2005 - Mar 2006.
Kyushu University, Fukuoka, Japan,	Nov 2004 - Dec 2004.
University of Waterloo, Waterloo, Canada,	Aug 2004 - Sep 2004.
Korea University, Seoul, South Korea,	Jan 2004 - Mar 2004.

Industrial Experiences

Software Analyst
Multinational Company **Cognizant Technological Solution** Feb 2002 - Jun 2002.

Stock Market Analyst
East India Security, National Stock Exchange. Aug 2001 - Jan 2002.

Teaching Experience

1. M.Math 2nd Year **Probability Theory** (July-2011- Dec-2011).
2. Series of lectures on **Probability Theory** at C R Rao AIMSCS (Jan 2011 - May 2011).
3. Series of lectures on **Basic Theory of Cryptography** at the George Washington University (Jan 2010 - Apr 2010).
4. Grad course in **Algebra** in Fall (Sept 2007- Dec 2007) at CINVESTAV.
5. Grad course **Probability Theory** in Fall (Sept 2007- Dec 2007) at CINVESTAV.
6. **Combinatorics** at the Training Camp for Indian National Mathematical Olympiad 2007.
7. Undergraduate course in **Algebra** (Math135) during Fall 2006 at the University of Waterloo.
8. Organized **Hash study group** and delivered series of seminars with Professor Alfred Menezes and Professor Douglas R. Stinson at the University of Waterloo from May 2006 to Aug 2006.
9. Part time course with Prof Bimal Roy in **Cryptography** for Master Degree students at Indian Statistical Institute - 2003.
10. **Algebraic Geometry Coding Theory** series of classes at the Applied Statistics Unit, Indian Statistical Institute, Kolkata.

Invited Talks

University of Luxemburg in Luxemburg,	Mar 2009
FSE in Leuven, Belgium	Feb 2009
University of Trento in Trento,	May 2007.
University of Calgary in Calgary,	Mar 2007.
Indocrypt in Kolkata,	Dec 2006.
Asiacrypt in Shanghai,	Dec 2006.
Indocrypt in Bangalore,	Dec 2005.
Katholieke University Leuven in Leuven,	Feb 2005.
FSE in Paris,	Feb 2005.
SAC in Waterloo,	Aug 2004.
ACISP in Sydney,	Jul 2004.
Asiacrypt in Taipei,	Dec 2003.
IIT Mumbai in Mumbai,	May 2003.

Awards and other recognitions received:

1. **Indian National Mathematical Olympiad Awardee** and participant of **International Mathematical Olympiad Training Camp** in 1995 and 1996.
2. **Junior Research Fellowship** (CSIR, Government of India), 2001 and was selected among top three students for a prestigious Shyama-Prasad Scholarship.
3. Actively participated the first SHA-3 Hash workshop and a member of technical team of SHA-3 selection process in **NIST**.
4. One of the program committee members of the following well known cryptographic international conferences: Inscrypt, 2007-08, Indocrypt 2009-10, IWSEC 2009.
5. Erdȯs number is two.

Field of Specialization

Cryptography and Its Applications.

Research Interest

My ongoing research is mainly focused on the design, cryptanalysis, security analysis of *hash function* and any kind of symmetric key security related topics (that includes security analysis of *pseudo random function, MAC, modes of operations* etc.). Very recently, I am interested in cryptographic protocols including e-voting.

Industrial experience

Experience in Indian Stock Market as a share market analyst. Later, worked in CTS as a software analyst and worked in a medical project.

Other related knowledge

1. Programming language : C, C++, Visual Basic, Fortran, VHDL etc.
2. Some database knowledge : RDBMS, oracle and SQL and database related to cryptography.
3. Statistical packages : Splus, SAS, SPSS.
4. Time-series data analysis : Eviews, Gate, Metastock for share market prediction and time series data analysis.
5. Mathematical packages : Maple, Mathematica.

Teaching Interest :

1. I can teach statistical courses. e.g. Basic Statistics, Estimation and Hypothesis testing, Design of Experiment, Linear Statistical Model etc.
2. I am also interested to take any graduate or undergraduate level mathematical courses for example, Algebra, Linear Algebra, Number Theory, Analysis, Calculus, Probability theory, Topology, Complex Analysis etc.
3. Besides mathematical courses, I would be able to teach some mathematics based computer science courses such as complexity theory, algorithmic number theory, cryptography, coding theory, finite field and its application.

Research Experience

Dr Mridul Nandi successfully defended his PhD thesis in cryptology in Jan 2006. During his PhD at Indian Statistical Institute, he published several research works in cryptography in Journals and Springer Verlag conference proceedings. Immediately after his PhD, Dr Nandi visited INRIA (Institut national de recherche en informatique et en automatique), Rocquencourt for three months, and then joined as a post doctoral fellow for one year at the University of Waterloo under supervision of Professor Douglas R Stinson, a well known researcher in the cryptographic community. After completion of his post-doc he visited Indian Statistical Institute and then joined to CINVESTAV, IPN in Mexico City as an Assistant Professor. Dr Mridul Nandi got a chance to work with U.S. government organization National Institute of Standards and Technology (NIST) as one of the member in the selection committee of SHA-3, a fututre standard for hash functions. He put a great effort to make a list of 14 candidates among 61. He also worked in The George Washington University, Washington D.C., U.S.A. as a Senior Research Associate for analyzing cryptographic voting protocol. He also proposed an enhanced e-voting scheme. Now Dr Mridul Nandi is affiliated with C R Rao AIMSCS, Hyderabad as an Associate Professor and devoted for cryptographic and related research works.

Thesis Topic

My thesis is based on analyzing hash functions in the view of different security notions. In my thesis, I have designed several hash function optimally secure against target collision attack. I have analyzed the generalized PGV hash families in black-box model. I have designed several double length hash functions which are important for large hash values. I have also showed how one can obtain efficiently multi-collision attacks on a wide class of hash functions.

Statement about research contribution

Hash function is an important building block in cryptography. Informally, it is a publicly and efficiently computable function from any arbitrary message into a small random looking binary string which can be thought of as a finger print of the message. MAC is also an authentication of a document, but the computation of authentication is based on a secret key. These are popular in many applications, like encryption, authenticated encryption, digital signature, digital time-stamping, message authentication, PKI or public key infrastructure etc.

During his doctoral research, Dr. Mridul Nandi studied the domain extension, range extension [10-14] of cryptographic hash function and universal one way hash function (UOWHF). UOWHF is a special kind of hash function which is useful in digital signature. Dr. Mridul Nandi proposed two efficient, parallel, mask based UOWHF. One of them was based on a complete binary tree [5, 14] which was very easy to implement and also was a reasonable improvement over the till date best known complete binary tree based extension. The second one was an optimal in a wide tree-based class [12]. He also provided a non-trivial sufficient condition for UOWHF [12]. He also studied UOWHF properties of PGV hash functions [4]. Multicollision is a generalization of collision which is an important security property of a hash function. **Dr. Nandi provided a multicollision attack on generalized Merkle-Damgård hash function [3] (this work was done during his PhD**

and it was being included in his thesis, but it was published when he was post-doc at Waterloo University).

Pseudorandom oracle (PRO) property, a close object to the random oracle, of a hash designs has nowadays become an important research area due to the SHA-3 competition a competition organized by NIST for the selection of the hash standard. Dr. Nandi et al. designed a fast wide-pipe hash[9] which was proved to be PRO and faster than popular wide-pipe hash function. The major part of this work, however, has been done abroad. To design a secure hash function with rate-1 (maximum efficiency) is hard. Dr. Nandi partially solved this direction of research during his PhD. He provided an almost optimum hash design [10] and a rate 2/3 hash function having good security [11].

Dr. Nandi has significant contribution in symmetric key encryption and authenticated encryption, providing improved security analysis and proposing a generic method to enrich message space[3] of wide-block encryption. More precisely, given an encryption scheme which can encrypt a full block messages, he has given a method for obtaining an encryption which can encrypt messages of any sizes, including partial block messages. Dr. Nandi has demonstrated an **improved security analysis** of most popular constructions of MAC like **OMAC** [1] or **CMAC**, which is a NIST standard. Thus CMAC guarantees more security than it was believed to have. As a continuation of this research he considered a general class of MAC and provided an improved security analysis [16]. However the work on generalization has been done while he was abroad.

Recently, he has also characterized the so-called Luby-Rackoff (LR) encryption completely and provided an optimum single key LR variant[8] (the major part of the work was done abroad).

List of Publications

International Journal Publications

[1]* **Mridul Nandi**.
An improved security analysis of OMAC.
Journal of Mathematical Cryptology. Volume 3, Issue 2, Pages 133 - 148, 2009.

[2] D. Chang, **M. Nandi**, J. Lee, J. Sung, S. Hong, J. Lim, H. Park and K. Chun
Compression Function Design Principles Supporting Variable Output Lengths from One Small Function. **IEICE Trans. Fundamentals**, volume 91-A, number 9, pp 2607 - 2614, 2008.

[3]* **M. Nandi** and A. Mandal.
An Improved Security Analysis of PMAC.
Journal of Mathematical Cryptology, Volume 2, Issue 2, pp 149 - 162, 2008.

[4] **Mridul Nandi**
A generic method to extend message space of a strong pseudorandom permutation. Special Issue on Applied Cryptography & Data Security, **Journal of "Computacion y Sistema"**, vol 12, no 3, pp 285 - 296, 2008.

[5]* **Mridul Nandi** and D. R. Stinson.
Multicollision attacks on a class of generalized hash functions. **IEEE Transactions on Information Theory** volume 53 - 2, pp 759 - 767, 2007. (this work is completely included in PhD thesis of Dr Mridul Nandi and published later while he was at Waterloo University)

[6] W. Lee, **Mridul Nandi**, P. Sarkar, D. Chang, S. Lee and K. Sakurai.
PGV-style Block-Cipher-Based Hash Families and Black-Box Analysis. **IEICE transaction on Fundamentals**, vol E88-A, no.1, pp. 39 - 48, January 2005.

[7] W. Lee, D. Chang, S. Lee, S. H. Sung, and **Mridul Nandi**.
Construction of UOWHF : Two New Parallel Methods. **IEICE transaction on Fundamentals**, vol E88-A, no.1, pp. 49 - 58, January 2005.

Springer Published Proceedings

[8] Donghoon Chang, **Mridul Nandi**, Moti Yung:
On the Security of Hash Functions Employing Blockcipher Postprocessing. FSE 2011, Volume 6733, pp 146-166, 2011.

[9] David Chaum, Alex Florescu, **Mridul Nandi**, Stefan Popoveniuc, Jan Rubio, Poorvi L. Vora, Filip Zagorski. *Paperless Independently-Verifiable Voting*, to be published in VoteID 2011, LNCS 2011.

[10]* **Mridul Nandi**.
The Characterization of Luby-Rackoff and Its Optimum Single-Key Variants. **Indocrypt** 2010, Lecture Notes in Computer Science, Volume 6498, pp 82 - 97, 2010.

[11] **Mridul Nandi** and Souradyuti Paul.
Speeding Up The Wide-pipe: Secure and Fast Hashing. **Indocrypt** 2010, Lecture Notes in Computer Science, Volume 6498, pp 144 - 162, 2010.

[12] **Mridul Nandi**, Stefan Popoveniuc and Poorvi Vora.
Stamp-It: A Method for Enhancing Universal Verifiability. To appear in **ICISS** 2010.

[13]* **Mridul Nandi**.
A Unified Method for Improving PRF Bounds for a Class of Blockcipher based MACs. **Fast Software Encryption** 2010. Springer, volume 6147, pp 212-219, 2010.

[14] Rishiraj Bhattacharyya, Avradip Mandal, and **Mridul Nandi**.
Security Analysis of the Mode of JH Hash Function. **Fast Software Encryption** 2010. Springer, volume 6147, pp 168-191, 2010.

[15] Rishiraj Bhattacharya, Avradip Mandal, **Mridul Nandi**.
Indifferentiability Characterization of hash functions and Optimal Bounds of Popular Domain Extensions. Progress in Cryptology - **Indocrypt** 2009, volume 5922, pp 199- 218, 2009.

[16] **Mridul Nandi**
Characterizing Padding Rules of MD Hash Functions Preserving Collision Security.
Information Security and Privacy, 14th Australasian Conference, volume 5594, pp 171 - 184, 2009.

[17]* **Mridul Nandi**
Fast and Secure CBC-type MAC Algorithms.
Fast Software Encryption, 16th International Workshop, volume 5665, pp 375 - 393, 2009.

[18] **Mridul Nandi**
A Simple Security Analysis of Hash-CBC and a New Efficient One-Key Online Cipher.
Progress in Cryptology-**Indocrypt** 2008. Volume 5365/2008, pp 350 - 362, 2008.

[19] Debrup Chakrabarty and **Mridul Nandi**
An improved security analysis of HCTR. **Fast Software Encryption** 2008, Springer, Lecture Notes in Computer Science, volume 5086, pp 289 - 302, 2008.

[20] Donghoon Chang and **Mridul Nandi**

Improved indifferentiability security analysis of chopMD Hash Function. **Fast Software Encryption** 2008, Springer, Lecture Notes in Computer Science, volume 5086, pp 429-443, 2008.

[21] Donghoon Chang, Sangjin Lee, **Mridul Nandi** and Moti Yung.
Indifferentiable Security Analysis of Popular Hash Function with prefix-free padding. **Asiacrypt** 2006. Volume 4284/2006, pp 283 - 289, 2006.

[22] **Mridul Nandi**.
A Simple and Unified Method of Proving Indistinguishability. **Indocrypt** 2006. Volume 4329/2006, pp 317 -334, 2006.

[23] Donghoon Chang, Kishan Chand Gupta and **Mridul Nandi**.
RC4-Hash : A New Hash Function based on RC4. **Indocrypt** 2006. Volume 4329/2006, pp 80 - 94, 2006.

[24] **Mridul Nandi**
Towards optimal double-length domain extension. **Indocrypt** 2005, Volume 3797/2005, pp 77 - 89, 2005.

[25] **Mridul Nandi**, Wonil Lee, Kouichi Sakurai and Sangjin Lee.
Security analysis of a rate 2/3 *double length hash function in the black box model*, **Fast Symmetric Encryption** 2005. Volume 3557/2005, 243 - 254, 2005.

[26] **Mridul Nandi**.
A Sufficient Condition on Domain Extension of UOWHF, Proceedings of **Selected Areas in Cryptography** 2004. Volume 3357/2004, pp 341 - 354, 2004.

[27] Wonil Lee, **Mridul Nandi**, Palash Sarkar, Donghoon Chang, Sangjin Lee and Kouichi Sakurai.
A Generalization of PGV Hash Functions and Its Security Analysis in Black-Box Model, Proceedings of **Australasian Conference on Information Security and Privacy** 2004. Volume 3108/2004, pp 212 - 223, 2004.

[28] Wonil Lee, Donghoon Chang, Sangjin Lee, Soohak Sung and **Mridul Nandi**.
New parallel tree based constructions of UOWHF, Proceedings of **Asiacrypt** 2003. Volume 2894/2003, pp 208 -227, 2003.