Curriculum Vitae of Mridul Nandi 3rd July 2020

Proforma

1. Name: Mridul Nandi
2. Designation: Professor, Indian Statistical Institute
3. Date of Birth: 21st June 1977
4. Date of Last Promotion / Appointment: 1st January 2020 as a Full-time Professor.
5. Details of Educational Qualification:
   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, Ex-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 76.1%

   3. **B.Stat.** (Bachelor Degree in Statistics) **1996 - 1999**
   Indian Statistical Institute
   First division with distinction 76.85%

Achievements / Work done 1st August 2015 onwards

1.a Students Supervised (completed)

1. Nilanjan Datta: **PhD Thesis** on Pseudorandom Function and Authenticated Encryption. Obtained Ph.D. in 2016.
2. Avik Chakraborty: **PhD Thesis** on Design, Analysis and Hardware Implementation of Authenticated Encryption Schemes. Obtained Ph.D. in 2017.
3. Ritam Bhaumik: **PhD Thesis** on Design and Provable Security Analysis of Symmetric Key Modes. Obtained Ph.D. in 2020.
4. Avijit Dutta: **PhD Thesis** on Design and Analysis of Beyond Birthday Secure Message Authentication Codes. Obtained Ph.D. in 2020.
5. Ashwin Jha: **PhD Thesis** on Provable security on Pseudorandom Functions. Obtained Ph.D. in 2020.

1.b. On-going PhD Students Supervising

1. Soumya Chattopadhyay on Provable security on PMAC type designs
2. Suprita Talnikar on Provable Security on Permutation vased Designs
3. Biswajit Chakraborty on Lightweight Authenticated Encryptions
4. Anik Raychaudhuri on Hash Functions
5. Arghya Bhattacharjee on Lightweight Authenticated Encryptions and Cryptanalysis
6. Snehal Mitrogi on Cryptanalysis on Designs
7. Debasmita Chakraborty on Cryptanalysis on AES
8. Abishanka Saha On a Lower Bounds of Proximity of Function Class

9. Sayantan Paul on Differential Privacy and Data Anonymisation
10. Chandranan Dhar on Communication Complexity and Time-Memory Trade-Off.

2. Teaching Experience

1. **Cryptology** M.Tech CS, 2nd Year First Semester of 2019-2020.
2. **Basic Probability Theory** M.Math 2nd Year First Semester of 2019-2020.
3. **Advanced Cryptology** M.Tech CS, 2nd Year Second Semester of 2018-2019.
4. **Cryptology** M.Tech CS, 2nd Year First Semester of 2018-2019.
5. **Algebra and Number Theory** M.Tech CrS, 1st Year First Semester of 2017-2018.
6. A series of lectures on **Coefficient H-Technique** for research scholars, July 2018- Aug 2018.
7. **Number Theory** B.Stat 3rd Year Second Semester of 2017-2018.
8. **Cryptology** M.Tech CS, 2nd Year First Semester of 2017-2018.
9. **Number Theory** B.Stat 3rd Year Second Semester of 2016-2017.
10. A series of lectures on **Provable security of symmetric key** for research scholars, Sept 2016- Nov 2016.
11. **Abstract Algebra** B.Stat 2nd Year First Semester of 2016-2017.
12. **Graph Theory and Combinatorics** M.Math 2nd Year Second Semester of 2015-16.
13. **Basic Probability Theory** M.Math 2nd Year July 2015- Dec 2015.

3. Awards and other recognitions received (in Last 5 Years):

1. **Invited as a keynote speaker** at Current Trends in Cryptology 2020 workshop (www.ctcrypt.ru).
2. **Program co-chair** of SPACE 2019
3. Designer of **COLM** which is selected as a **winner of CAESAR** authenticated encryption algorithm in *Defense in depth* category.
4. **Program co-chair** of Asian Symmetric Key Workshop 2018.
5. **Invited as a keynote speaker** of Indocrypt 2018 (will be held on Dec. 2018).
6. **Invited as a keynote speaker** of SPACE 2018 (will be held on Dec. 2018).
7. **Invited Speaker** for Asian Symmetric Key Workshop 2017.
8. **Invited Speaker** for Asian Symmetric Key Workshop 2016.
9. **Invited Speaker** for Asian Symmetric Key Workshop 2015.
10. **Regional Mathematical Olympiad Coordinator** for West Bengal Region (2017, 2018, 2019 and 2020)

4. Recognized Algorithms Designed

1. ELmD (with Nilanjan Datta): A misuse resistant authenticated encryption. Submitted to CAESAR competition, 2014. Currently named as COLM after merging with COPA and selected as one of the winners in "defense in depth" category of CAESAR. This work is also invited for publication of a special issue on Journal of Cryptology (submission in 2019).
2. **COFB** (with Avik Chakraborty, Tetsu Iwata and Kazuhiko Minematsu). *It was selected as one of the best papers in CHES 2017 and invited for publication of Journal of Cryptology (Accepted in 2019).*
3. Designers of the following algorithms selected for the second round of Lightweight Authenticated Encryption and Hash Algorithms for NIST Standard (https://csrc.nist.gov/Projects/Lightweight-Cryptography).
   (1) COMET (2) ESTATE (3) GIFT-COFB (4) HyENA (5) LOTUS-AEAD and LOCUS-AEAD (6) mixFeed (7) ORANGE (8) ORIBATIDA (9) PHOTON-Beetle and (10) SPOC.

   All **10 algorithms have been selected for the second round** (consisting of 32 algorithms).
   https://csrc.nist.gov/News/2019/lightweight-cryptography-round-2-candidates

5.a. International Journal Publications (reverse order in last 5 years)

[35] Bishwajit Chakraborty, Ashwin Jha, **Mridul Nandi**. On the Security of Sponge-type Authenticated Encryption Modes. Accepted for **IACR Trans. Symmetric Cryptology**. Volume 2020(2).

[34] Avik Chakraborti, **Mridul Nandi**, Suprita Talnikar, Kan Yasuda. On the Composition of Single-Keyed Tweakable Even-Mansour for Achieving BBB Security. Accepted for **IACR Trans. Symmetric Cryptology**. Volume 2020(2).

[33] Ashwin Jha, **Mridul Nandi**. Tight Security of Cascaded LRW2, **Journal of Cryptology** volume 33, pages 1272-1317 (2020).

[32] Avik Chakraborti, Nilanjan Datta, Ashwin Jha, Cuauhtemoc Mancillas-Lpez, **Mridul Nandi**, Yu Sasaki, ESTATE: A Lightweight and Low Energy Authenticated Encryption Mode. **IACR Trans. Symmetric Cryptology**. Volume 2020, Special Issue 1, pp 350-389

[31] Avik Chakraborti, Nilanjan Datta, Ashwin Jha, Snehal Mitragotri, **Mridul Nandi**. From Combined to Hybrid: Making Feedback-based AE even Smaller. **IACR Trans. Symmetric Cryptology**. Volume 2020, Special Issue 1, pp 417-445

[30] **Mridul Nandi**, Tapas Pandit: Delegation-based conversion from CPA to CCA-secure predicate encryption. IJACT 4(1): 16-35 (2020)

[29] **Mridul Nandi** and Tapas Pandit. Efficient fully CCA-secure predicate encryptions from pair encodings. Accepted in AMC (in press)

[28] Avik Chakraborti, Nilanjan Datta, Ashwin Jha, Cuauhtemoc Mancillas-Lpez, **Mridul Nandi**, Yu Sasaki. INT-RUP Secure Lightweight Parallel AE Modes. **IACR Trans. Symmetric Cryptology**. 2019(4). pp 81-118.

[27] Ashwin Jha; Cuauhtemoc Mancillas-Lopez; **Mridul Nandi**; Sourav Sen Gupta. On random access of OCB. To appear in **IEEE Transaction on Information Theory** 2019.

[26] Tony Grochow; Eik List; **Mridul Nandi**. DoveMAC: A TBC-based PRF with Smaller State, Full Security, and High Rate. To appear in **IACR Trans. Symmetric Cryptology**. 2019(4).

[25] Avik Chakraborti, Tetsu Iwata, Kazuhiko Minematsu, **Mridul Nandi**.
Blockcipher-based Authenticated Encryption: How Small Can We Go? **Journal of Cryptology**, May 2019.

[24] Nilanjan Datta, Avijit Dutta, **Mridul Nandi**, Kan Yasuda. DWCDM+: A BBB Secure Nonce Based MAC, Accepted in a special issue of **AMC**, 2019

[23] **Mridul Nandi**, Tapas Pandit. Delegation-based conversion from CPA to CCA-secure predicate encryption, **International Journal of Applied Cryptography**, 2019.

[22] Debapriya BasuRoy, Avik Chakraborti, Donghoon Chang, S V Dilip Kumar, Debdeep Mukhopadhyay, **Mridul Nandi**. Two Efficient Fault Based Attacks on CLOC and SILC. **Journal of Hardware and Systems Security**, September 2017, Volume 1, Issue 3, pp 252 - 268.

[21] Avik Chakraborti, Nilanjan Datta, **Mridul Nandi**. Optimum no. of non-linear computations for symmetric key modes. Accepted in **J. Mathematical Cryptology** 2018.

[19] Nilanjan Datta; Avijit Dutta; **Mridul Nandi**; Goutam Paul. Double-block Hash-then-Sum: A Paradigm for Constructing BBB Secure PRF. **IACR Trans. Symmetric Cryptology**. 2018(3).

[18] **Mridul Nandi**, Tapas Pandit. Verifiability-based conversion from CPA to CCA-secure predicate encryption. **Appl. Algebra Eng. Commun. Comput.** 29(1): 77-102 (2018)

[17] Ashwin Jha, **Mridul Nandi**. On rate-1 and beyond-the-birthday bound secure online ciphers using tweakable block ciphers. **Cryptography and Communications** 10(5): 731-753 (2018)

[16] Srimanta Bhattacharya, **Mridul Nandi**. A note on the chi-square method: A tool for proving cryptographic security. **Cryptography and Communications** 10(5): 935-957 (2018)

[15] Avik Chakraborti, Anupam Chattopadhyay, Muhammad Hassan, **Mridul Nandi**. TriviA and uTriviA: two fast and secure authenticated encryption schemes. **J. Cryptographic Engineering** 8(1): 29-48 (2018)

[14] Avik Chakraborti, Nilanjan Datta, **Mridul Nandi**, Kan Yasuda. Beetle Family of Lightweight and Secure Authenticated Encryption Ciphers. **IACR Trans. Cryptographic Hardware Embedded System**. 2018(2): 218-241 (2018)

[13] Srimanta Bhattacharya, **Mridul Nandi**. Revisiting Variable Output Length XOR Pseudorandom Function. **IACR Trans. Symmetric Cryptology** 2018(1): 314-335 (2018)

[12] Shoni Gilboa, Shay Gueron, **Mridul Nandi**. Balanced Permutations Even-Mansour Ciphers. **Cryptography** 1(1): 2 (2017)

[11] Ashwin Jha, Avijit Dutta, **Mridul Nandi**. A New Look at Counters: Don't Run Like Marathon in a Hundred Meter Race. **IEEE Transaction on Computers**. 66(11): 1851-1864 (2017)

[10] Nilanjan Datta, Atul Luykx, Bart Mennink, **Mridul Nandi**. Understanding RUP Integrity of COLM. **IACR Trans. Symmetric Cryptology**. 2017(2) 143-161 (2017)

[9] Elena Andreeva; Guy Barwell, Ritam Bhaumik, **Mridul Nandi**, Dan Page, Martijn Stam. Turning Online Ciphers Off. **IACR Trans. Symmetric Cryptology** 2017(2) 105-142 (2017)

[8] Ashwin Jha, Avradip Mandal, **Mridul Nandi**. On The Exact Security of Message Authentication Using Pseudorandom Functions. **IACR Trans. Symmetric Cryptology**. 2017(1): 427-448

(2017)

[7] Nilanjan Datta, Avijit Dutta, **Mridul Nandi**, Goutam Paul, Liting Zhang: Single Key Variant of PMAC_Plus. **IACR Trans. Symmetric Cryptology** 2017(4): 268-305 (2017)

[6] Ashwin Jha, Avijit Dutta, **Mridul Nandi**. Tight Security Analysis of EHtM MAC. **IACR Trans. Symmetric Cryptology** 2017(3): 130-150 (2017)

[5] Eik List, **Mridul Nandi**. ZMAC+ - An Efficient Variable-output-length Variant of ZMAC. **IACR Trans. Symmetric Cryptology**. 2017(4): 306-325 (2017)

[4] Ritam Bhaumik, **Mridul Nandi**. OleF: an Inverse-Free Online Cipher. An Online SPRP with an Optimal Inverse-Free Construction. **IACR Trans. Symmetric Cryptology**. 2016(2): 30-51 (2016)

[3] Ashwin Jha, **Mridul Nandi**.
Revisiting Structure Graphs: Applications to CBC-MAC and EMAC. **J. Mathematical Cryptology** 10(3-4): 157-180 (2016)

[2] **Mridul Nandi**, Tapas Pandit. On the Security of Joint Signature and Encryption Revisited. **J. Mathematical Cryptology** 10(3-4): 181-221 (2016)

[1] Lilian Bossuet, Nilanjan Datta, Cuauhtemoc Mancillas-Lpez, **Mridul Nandi**. ELmD:
A Pipelineable Authenticated Encryption and Its Hardware Implementation. **IEEE Trans Computers** 65(11): 3318-3331 (2016)

5.b. IACR Conferences in reverse order

[14] **Mridul Nandi**. Mind the Composition: Birthday Bound Attacks on EWCDMD and SoKAC21. EUROCRYPT (1) 2020: 203-220

[13] Avijit Dutta, **Mridul Nandi**, Suprita Talnikar: Beyond Birthday Bound Secure MAC in Faulty Nonce Model. **EUROCRYPT 2019**

[12] **Mridul Nandi**. Bernstein Bound on WCS is Tight - Repairing Luykx-Preneel Optimal Forgeries. **CRYPTO 2018**

[11] Gatan Leurent, **Mridul Nandi**, Ferdinand Sibleyras: Generic Attacks against Beyond-Birthday-Bound MACs. **CRYPTO 2018**

[10] Nilanjan Datta, Avijit Dutta, **Mridul Nandi**, Kan Yasuda: Encrypt or Decrypt? To Make a Single-Key Beyond Birthday Secure Nonce-Based MAC. **CRYPTO 2018**

[9] Srimanta Bhattacharya, **Mridul Nandi**: Full Indifferentiable Security of the Xor of Two or More Random Permutations Using the χ^2 Method. **EUROCRYPT 2018**: 387-412

[8] Yu Long Chen, Bart Mennink, **Mridul Nandi**: Short Variable Length Domain Extenders with Beyond Birthday Bound Security. **ASIACRYPT** (1) 2018: 244-274

[7] Ritam Bhaumik, Eik List, **Mridul Nandi**: ZCZ - Achieving n-bit SPRP Security with a Minimal Number of Tweakable-Block-Cipher Calls. **ASIACRYPT** (1) 2018: 336-366

[6] Ritam Bhaumik; **Mridul Nandi**. Improved Security for OCB3. **ASIACRYPT (2) 2017** 638-666.

[5] Ritam Bhaumik; Nilanjan Datta; Avijit Dutta; Nicky Mouha; **Mridul Nandi**. The Iterated Random Function Problem. **ASIACRYPT (2) 2017** 667-697

[4] Avik Chakraborti, Tetsu Iwata, Kazuhiko Minematsu, **Mridul Nandi**. Blockcipher-based Authenticated Encryption: How Small Can We Go? **CHES 2017**

[3] **Mridul Nandi**. On the Optimality of Non-Linear Computations of Length-Preserving Encryption Schemes.**ASIACRYPT (2) 2015**: 113-133

[2] Ritam Bhaumik, **Mridul Nandi**. An Inverse-Free Single-Keyed Tweakable Enciphering Scheme. **ASIACRYPT (2) 2015**: 159-180

[1] Avik Chakraborti, Anupam Chattopadhyay, Muhammad Hassan, **Mridul Nandi**. TriviA: A Fast and Secure Authenticated Encryption Scheme. **CHES 2015**: 330-353

5.c. Others LNCS Proceedings in reverse order

[8] Avijit Dutta, **Mridul Nandi**. BBB Secure Nonce Based MAC Using Public Permutations. **AFRICACRYPT** 2020: pp 172-191

[7] Avijit Dutta, **Mridul Nandi**. Tweakable HCTR: A BBB Secure Tweakable Enciphering Scheme. **INDOCRYPT** 2018: 47-69

[6] Ashwin Jha and Eik List and Kazuhiko Minematsu and Sweta Mishra and **Mridul Nandi**. XHX - A Framework for Optimally Secure Tweakable Block Ciphers from Classical Block Ciphers and Universal Hashing. **Latincrypt 2017**: 207–227.

[5] Avik Chakraborti, Nilanjan Datta, **Mridul Nandi**: Practical Fault Attacks on Minalpher: How to Recover Key with Minimum Faults? **SPACE 2017**: 111-132

[4] Eik List, **Mridul Nandi**. Revisiting Full-PRF-Secure PMAC and Using It for Beyond-Birthday Authenticated Encryption.**CT-RSA 2017**: 258-274

[3] Avik Chakraborti, Nilanjan Datta, **Mridul Nandi**.
INT-RUP Analysis of Block-cipher Based Authenticated Encryption Schemes. **CT-RSA 2016**: 39-54

[2] Debapriya Basu Roy, Avik Chakraborti, Donghoon Chang, S. V. Dilip Kumar, Debdeep Mukhopadhyay, **Mridul Nandi**.
Fault Based Almost Universal Forgeries on CLOC and SILC. **SPACE 2016**: 66-86

[1] Avijit Dutta, **Mridul Nandi**, Goutam Paul.
One-Key Compression Function Based MAC with Security Beyond Birthday Bound. **ACISP (1) 2016**: 343-358

6. Books Edited

Shivam Bhasin, Avi Mendelson, **Mridul Nandi**. Security, Privacy, and Applied Cryptography Engineering - 9th International Conference, SPACE 2019, Gandhinagar, India, December 3-7, 2019, Proceedings. Lecture Notes in Computer Science 11947, Springer 2019, ISBN 978-3-030-35868-6.

Achievements / Work done before 31st July 2015

Training Programs

1. Organizing Winter School in 2014 Dec at ASU on Interplay between Statistics and Cryptology.
2. Organizing Workshop on SHA3 and Its evaluation on 2012 Dec.

Awards and other recognitions received:

1. Invited Speaker for ASK 2014.
2. Program co-Chair of Indocrypt 2012 (jointly with Stvenn Galbraith).
3. **Indian National Mathematical Olympiad Awardee** and participant of **International Mathematical Olympiad Training Camp** in 1995 and 1996.
4. **Junior Research Fellowship** (CSIR, Government of India), 2001 and was selected among top three students for a prestigious Shyama-Prasad Scholarship.
5. A Member of Selection Committee of SHA3 by **NIST** (An US Federal Government Project).
6. Erdȯs number is two (co-authored with Douglas Stinson).

Books Edited

[1] Indocrypt 2013, Lecture Notes in Computer Science, Springer Verlag, Volume No. 7668

Recognized Algorithms Designed

1. TriviA (with Avik Chakraborty): A streamcipher based authenticated encryption. Submitted to CAESAR competition, 2014. It was selected for the second round.

Teaching Experience

1. **Advanced Cryptology** M.Tech 2nd Year Jan 2015 - April 2015.
2. **Cryptology** M.Tech 2nd Year Aug 2014 - Dec 2014.
3. **Advanced Cryptology** M.Tech 2nd Year Jan 2014 - April 2014.
4. **Basic Probability Theory** M.Math 2nd Year July 2013- Dec 2013.
5. **Abstract Algebra** B.Stat 2nd Year Jan 2013- April 2013.
6. **Probability and Stochastic Process** for M.Tech 1st year July 2012-Dec 2012.
7. **Linear Algebra-II** B.Stat 1st Year Jan 2012- April 2012.
8. M.Math 2nd Year **Probability Theory** (July-2011- Dec-2011).
9. Series of lectures on **Probability Theory** at C R Rao AIMSCS (Jan 2011 - May 2011).
10. Series of lectures on **Basic Theory of Cryptography** at the George Washington University (Jan 2010 - Apr 2010).
11. Grad course in **Algebra** in Fall (Sept 2007- Dec 2007) at CINVESTAV.
12. Grad course **Probability Theory** in Fall (Sept 2007- Dec 2007) at CINVESTAV.
13. **Combinatorics** at the Training Camp for Indian National Mathematical Olympiad 2007.
14. Undergraduate course in **Algebra** (Math135) during Fall 2006 at the University of Waterloo.
15. 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.
16. Part time course with Prof Bimal Roy in **Cryptography** for Master Degree students at Indian Statistical Institute - 2003.
17. **Algebraic Geometry Coding Theory** series of classes at the Applied Statistics Unit, Indian Statistical Institute, Kolkata.

International Journal Publications

[8] Debrup Chakraborty, **Mridul Nandi**.
Attacks on the Authenticated Encryption Mode of Operation PAE. **IEEE Trans**. Information Theory 61(10): 5636-5642 (2015)

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

[6] 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.

[5] **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.

[3] **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)

[2] 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.

[1] 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.

LNCS Proceedings in reverse order

[29] **Mridul Nandi**: Forging Attacks on Two Authenticated Encryption Schemes COBRA and POET. **ASIACRYPT (1) 2014**: pp 126-140

[28] **Mridul Nandi**: : XLS is Not a Strong Pseudorandom Permutation. **ASIACRYPT (1) 2014**: 478-490

[27] **Mridul Nandi**: *On the Minimum Number of Multiplications Necessary for Universal Hash Constructions.* IACR Cryptology ePrint Archive 2013: 574 (2013), **FSE 2014**.

[26] Nilanjan Datta, **Mridul Nandi**. *Misuse Resistant Parallel Authenticated Encryptions.* **ACISP 2014**, LNCS proceedings, pp 306-321, IACR Cryptology ePrint Archive 2013: 767 (2013).

[25] Mohammad A. AlAhmad, Imad Fakhri Alshaikhli, **Mridul Nandi**: Joux multicollisions attack in sponge construction. **Security of Information and Networks 2013**: 292-296

[24] David Chaum, Alex Florescu, **Mridul Nandi**, Stefan Popoveniuc, Jan Rubio, Poorvi L. Vora and Filip Zagrski. *Paperless Independently-Verifiable Voting.* **VoteID 2011**. LNCS Volume 7187, 2012, pp 140-157

[23] Nilanjan Datta, **Mridul Nandi**: Characterization of EME with Linear Mixing. **IWSEC 2014**, LNCS proceedings, pp 221 - 239, IACR Cryptology ePrint Archive 2014: 9 (2014)

[22] Nilanjan Datta, **Mridul Nandi**: Equivalence between MAC and PRF for Blockcipher based Constructions. **Provsec 2014**, pp 300 - 308, LNCS proceedings, pp- IACR Cryptology ePrint Archive 2013: 575 (2013)

[21] David Chaum, Alex Florescu, **Mridul Nandi**, Stefan Popoveniuc, Jan Rubio, Poorvi L. Vora and Filip Zagrski. *Paperless Independently-Verifiable Voting.* VoteID 2011. LNCS Volume 7187, 2012, pp 140-157

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

[19]* **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.

[18] **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.

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

[16] **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.

[15] 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.

[14] 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.

[13] **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.

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

[11] **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.

[10] 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.

[9] 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.

[8] 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.

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

[6] 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.

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

[4] **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.

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

[2] 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.

[1] 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.