Curriculum Vitae

Somindu C. Ramanna

Assistant Professor
Department of Computer Science and Engineering
Indian Institute of Technology
Kharagpur

Email: somindu.cr@gmail.com, somindu@cse.iitkgp.ac.in
Homepage: http://cse.iitkgp.ac.in/~somindu/

1 Professional Background

- 8th August 2018 – Present: Assistant Professor Grade-I, Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur.
- 3rd July 2017 – 7th August 2018: Assistant Professor on Tenure Track, Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur.
- 27th January 2017 – 30th June 2017: Assistant Professor (on Contract), School of Electrical Sciences, Indian Institute of Technology Bhubaneswar.
- 4th Feb 2015 – 30th Nov 2016: Post-doctoral researcher in the AriC team, LIP laboratory, École Normale Supériure de Lyon, France hosted by Dr. Benoît Libert (under project PALSE).

2 Academic Degrees

- **Doctor of Philosophy** from the Indian Statistical Institute, Kolkata in 2015.
  Supervised by Prof. Palash Sarkar, Applied Statistics Unit, Indian Statistical Institute.

  The main focus of my thesis was construction of efficient asymmetric pairing-based constructions of identity-based encryption (IBE) and related primitives within the dual system encryption framework. The related primitives include hierarchical IBE, identity-based broadcast encryption and attribute-based encryption over a sub-class of regular languages.
- **Master of Technology in Computer Science** from the Indian Statistical Institute, Kolkata in 2009.

  For the dissertation (supervised by Prof. Palash Sarkar), I worked on the problem of analysing multi-collision resistance of concrete hash functions against generalised birthday attacks.
- **Bachelor of Engineering in Information Science and Engineering** from Visveswaraiah Technological University, Belgaum, Karnataka in 2007.

3 Research Interests

- Public key cryptography
- Hash functions
- Pairing-based constructions of cryptographic primitives
- Foundations of lattice-based cryptography
- Pseudorandomness and complexity theory
- Efficient implementation of cryptographic algorithms and protocols

4 Publications/Preprints

Journals

1. Somindu C. Ramanna, Palash Sarkar. Efficient Adaptively Secure IBBE from the SXDH Assumption. IEEE Transactions on Information Theory 62(10): 5709–5726 (2016).

2. Somindu C. Ramanna and Palash Sarkar. On Quantifying the Resistance of Concrete Hash Functions to Generic Multi-Collision Attacks. In IEEE Transactions on Information Theory, 57(7): 4798–4816 (2011).

Peer-Reviewed Conferences

3. Sikhar Patranabis, Debdeep Mukhopadhyay and Somindu C. Ramanna. Function Private Predicate Encryption for Low Min-Entropy Predicates. To appear in PKC 2019.

4. Junqing Gong, Benoît Libert and Somindu C. Ramanna. Compact IBBE and Fuzzy IBE from Simple Assumptions. SCN 2018, LNCS Volume 11035, pp. 563–582.

5. Jie Chen, Benoît Libert and Somindu C. Ramanna. Non-Zero Inner Product Encryption with Short Ciphertexts and Private Keys. SCN 2016, LNCS Volume 9841, pp. 23–41.

6. Benoît Libert, Somindu C. Ramanna and Moti Yung. Functional Commitment Schemes: From Polynomial Commitments to Pairing-Based Accumulators from Simple Assumptions. ICALP 2016, LIPIcs Volume 55, pp. 30:1–30:14.

7. Somindu C. Ramanna. More Efficient Constructions for Inner-Product Encryption. ACNS 2016, LNCS Volume 9696, pp. 231–248.

8. Somindu C. Ramanna and Palash Sarkar. (Anonymous) Compact HIBE From Standard Assumptions. ProvSec, 2014. LNCS Volume 8782, pp. 243–258.

9. Somindu C. Ramanna and Palash Sarkar. Anonymous Constant-Size Ciphertext HIBE from Asymmetric Pairings. IMA Conference on Cryptography and Coding 2013. LNCS Volume 8308, pp. 344–363.

10. Somindu C. Ramanna, Sanjit Chatterjee and Palash Sarkar. Variants of Waters' Dual System Primitives Using Asymmetric Pairings - (Extended Abstract). Public Key Cryptography 2012. LNCS Volume 7293, pp. 298–315.

Technical Reports

11. Somindu C. Ramanna. Bounded DFA-Based Functional Encryption with Adaptive Security. IACR Cryptology ePrint Archive 2013/638, 2013.

5 Awards

Recipient of DST-Inspire Faculty Award, February 2017.

6 Teaching

1. **Computational Number Theory**, CS-Elective, January–April 2019 at IIT Kharagpur.

2. **Foundations of Cryptography**, CS-Elective, January–April 2019 at IIT Kharagpur.

3. **Theory of Computation**, B.Tech. (CS) 4th year, July–December 2018 at IIT Kharagpur.

4. **Programming and Data Structures Laboratory**, B.Tech. 1st year, July–December 2018 at IIT Kharagpur.

5. **Foundations of Cryptography**, CS-Elective, January–April 2018 at IIT Kharagpur.

6. **Programming and Data Structures Laboratory**, B.Tech. 1st year, January–April 2018 at IIT Kharagpur.
7. **Theory of Computation**, B.Tech. (CS) 4th year, will be teaching July–December 2017 jointly with Dr. Soumyajit Dey at IIT Kharagpur.
8. **Programming and Data Structures Laboratory**, B.Tech. 1st year, March–May at IIT Bhubaneswar.
9. **Advanced Cryptography**, Masters in Information Security and Risks 2nd year, October 2016 at ISFA, Université Lyon 1.
10. **Information Theory**, Masters in Computer Science 1st year, Sep–Dec 2015 at ENS de Lyon; Teaching Assistant with Dr. Omar Fawzi.
11. **C Programming and Data Structures**, B.Stat. 1st Year, Jul–Nov 2012 at ISI, Kolkata; jointly with Prof. Bimal Roy.
12. **Optimisation Techniques**, M.Tech.(CS) 1st Year, Jul–Nov 2011 at ISI, Kolkata; jointly with Prof. Bimal Roy.
13. **Database Management Systems**, B.Stat. 3rd Year, Jan–May 2010 at ISI, Kolkata; jointly with Prof. Subhamoy Maitra.

7 References

- **Prof. Palash Sarkar**, Applied Statistics Unit, Indian Statistical Institute, Kolkata.
  `palash@isical.ac.in`
- **Dr. Sanjit Chatterjee**, Department of Computer Science and Automation, Indian Institute of Science, Bengaluru.
  `sanjit@csa.iisc.ernet.in`
- **Dr. Benoît Libert**, Laboratoire LIP, École Normale Supériure, Lyon.
  `benoit.libert@ens-lyon.fr`
- **Prof. Damien Stehlé**, Laboratoire LIP, École Normale Supériure, Lyon.
  `damien.stehle@ens-lyon.fr`