CURRICULUM-VITAE

Rajeev Anand Sahu
Postdoctoral Researcher
Département d'Informatique
Université Libre de Bruxelles (ULB)
Office 2N8.207
Boulevard du Triomphe - CP212
B - 1050 Brussels
Belgium

RESEARCH INTERESTS

Elliptic Curve Cryptography, Post-Quantum Cryptography (Lattice-Based and Isogeny-Based), Digital Signature, Anonymity, Searchable Encryption, Attribute-Based Cryptography, Key Agreement Protocols.

EDUCATION

- **Ph.D. - Cryptography** May 2013
  MNNIT Allahabad, India
  Advisor : Dr. Sahadeo Padhye
- **Master of Science - Mathematics** May 2005
  GGDU Bilaspur, India
- **Bachelor of Science - Mathematics** May 2003
  GGDU Bilaspur, India

EXPERIENCE

- **Post-Doctoral Researcher** January 2017 - till date
  Université Libre de Bruxelles, Brussels, Belgium
  Supervisor: Prof. Olivier Markowitch
- **Assistant Professor** February 2016 - November 2016
  CRRao AIMSCS, UoH Campus, Hyderabad, India
- **Consultant** October 2012 - February 2016
  CRRao AIMSCS, UoH Campus, Hyderabad, India
- **Lecturer- Mathematics** August 2005 - December 2008
  National Institute of Technology Raipur, India.

COMPUTER SKILLS

PBC (Pairing Based Crypto), Sage.

BOOK AUTHORED

Introduction to Cryptography, CRC Press- Taylor & Francis Group (In Press).
with S. Padhye and V. Saraswat.

PUBLICATIONS (INTERNATIONAL JOURNALS)

1. A Secure Anonymous Proxy Signcryption Scheme, with V. Saraswat and A.K.Awasthi, Journal of Mathematical Cryptology, 11(2), 2017, pp. 63-84.
2. Efficient and Provable Secure Scheme for Delegation of Signing Rights between the Groups, with S. Padhye and N. Ojha, Annals of Telecommunications, Springer 2015, pp. 369-379.
3. Identity-Based Multi-proxy Multi-Signature Scheme Provable Secure in Random Oracle Model, with S. Padhye, Transactions on Emerging Telecommunications Technologies, Wiley, 2013. Vol 26, Issue 4, pp. 547-558.
4. Provable Secure Identity-Based Multi-proxy Signature Scheme, With S. Padhye, International Journal of Communication Systems, Wiley, 2013, Vol. 28, Issue 3, pp. 497-512.
5. Efficient ID-Based Proxy Multi-Signature Scheme Secure in Random Oracle, with S. Padhye, Frontiers of Computer Science, Springer, 2012, 6(4), pp. 421-428.

PUBLICATIONS (INTERNATIONAL CONFERENCES)

1. On New Zero-Knowledge Arguments for Attribute-Based Group Signatures from Lattices, With V. Kuchta, G. Sharma and O. Markowitch, International Conference on Information Security and Cryptology - ICISC 2017, Seoul, South Korea.
2. Multi-Party (Leveled) Homomorphic Encryption on Identity-Based and Attribute-Based Settings, With V. Kuchta, G. Sharma and O. Markowitch, International Conference on Information Security and Cryptology - ICISC 2017, Seoul, South Korea.
3. Generic Framework for Attribute-Based Group Signature, With V. Kuchta, G. Sharma and O. Markowitch, International Conference on Information Security Practice and Experience- ISPEC 2017, LNCS 10701, Springer, pp. 814-834.
4. Authenticated Group Key Agreement Protocol without Pairing, With G. Sharma, V. Kuchta, O. Markowitch and S. Bala, International Conference on Information and Communication Security- ICICS 2017, Beijing, China.
5. Short Integrated PKE+PEKS in Standard Model, With V. Saraswat, International Conference on Security, Privacy, and Applied Cryptography Engineering- SPACE 2017, LNCS 10662, Springer, pp. 226-246.
6. Secure Certificateless Proxy Re-encryption Without Pairing, With V. Kuchta, G. Sharma, T. Bhatia and O. Markowitch, International Workshop on Security- IWSEC 2017, LNCS 10418, Springer pp. 85-101.

7. Adaptively Secure Strong Designated Signature, with N. Sharma, V. Saraswat and B.K. Sharma, International Conference on Cryptology in India- INDOCRYPT 2016, LNCS 10095, Springer pp. 43-60.

8. Efficient Proxy Signature Scheme from Pairings, with F. Buccafurri and V. Saraswat, International Conference on Security and Cryptography- SECRYPT 2016, SCITEPRESS, pp. 471-476 .

9. Efficient and Secure Many-to-One Signature Delegation, with V. Saraswat, International Conference on Information and Communication Security- ICICS 2015, LNCS 9543, Springer, pp. 252-259.

10. Practical and Secure Integrated PKE+PEKS with Keyword Privacy, with F. Buccafurri, G. Lax and V. Saraswat, International Conference on Security and Cryptography- SECRYPT 2015, SCITEPRESS, pp. 448-453 .

11. Secure and Efficient Scheme for Delegation of Signing Rights, with V. Saraswat, International Conference on Information and Communication Security- ICICS 2014, LNCS 8958, Springer, pp. 258-273.

12. A Secure Anonymous Proxy Multi-signature Scheme, with V. Saraswat, International Conference on Security and Cryptography- SECRYPT 2014, SCITEPRESS, pp. 55-66.

RESEARCH PAPERS (IN SUBMISSION)

1. Lattice-Based Constrained Verifiable Random Function with Application to Non-Interactive Authenticated Key Exchange.

2. Identity-Based Strong Designated Verifier Group Signature.

3. A Twofold Group Key Agreement Protocol for NoC based MPSoCs.

4. Strong Designated Blind Signature.

RESEARCH PAPERS (IN PREPARATIONS)

1. Isogeny-based Post-quantum Strong Designated Verifier Blind Signature Scheme.

2. Secure and Efficient PKE+PEKS Scheme from Type 3 pairing.

STUDENT MENTORED

- Masters (at CRRao AIMSCS, Hyderabad, India) - 06
- Masters (at ULB, Brussels, Belgium) - 01 (ongoing)
- Bachelore (at ULB, Brussels, Belgium) - 01 (ongoing)

PROJECTS (Under Preparation)

- Efficient Cryptographic Protocols from Asymmetric Pairing.

AWARDS and SCHOLARSHIPS

- Stipend to attend the Workshop on Elliptic Curve Cryptography- ECC 2010 at Microsoft Research Redmond, Washington, USA.
- IEEE S&P Stipend to attend the IEEE Symposium on Security and Privacy 2011 at California, Berkeley USA.
- Qualcomm Stipend to attend the Eurocrypt 2012 at University of Cambridge, UK.
- NBHM International Travel Support by National Board for Higher Mathematics India to attend Eurocrypt 2012 at University of Cambridge, UK.
- Grant form Cryptology Research Society of India (CRSI) to present research paper in International Conference ICICS 2014 at University of Hong Kong.
- Stipend to attend Conference on Practice and Theory of Public-Key Cryptography- PKC 2015 at NIST, USA.
- Stipend to attend the Workshop on Elliptic Curve Cryptography- ECC 2017 at Radbound University, Nijmegen, The Netherlands.

PAST PROJECTS

- Side Channel Cryptanalysis — October 2012 - November 2016
- Post Quantum Cryptology — October 2014 - November 2016

TRAINING CONDUCTED

Team Leader for Training on Public Key Cryptosystems — July 2014

for scientists of the Cabinet Secretariat, New Delhi, India

REVIEWER

- Computers and Electrical Engineering (Elsevier)
- Journal of Hardware and System Security (Springer)
- International Journal of Communication Systems (Wiley)
- Journal of Information Security and Applications (Elsevier)

SUB REVIEWER

- ESORICS-2017
- SECRYPT-2017
- TRUSTBUS-2017

PROGRAM COMMITEE MEMBER

- ICICS 2015
- SPACE 2016

MEMBERSHIP IN SCIENTIFIC ORGANIZATIONS

- International Association of Cryptologic Research (IACR) Ref No. 20110125.
- Life member of Indian Mathematical Society (IMS), Membership No. S-10-32.
- Life member of Cryptology Research Society of India (CRSI), Membership No. L/300.

REFEREES

- **Dr. Olivier Markowitch**
  Associate Professor
  Département d'Informatique
  Université Libre de Bruxell, Brussels
  Belgium
  olivier.markowitch@ulb.ac.be
  Homepage: `https://www.ulb.ac.be/rech/inventaire/chercheurs/0/CH7840.html`
- **Dr. Vishal Saraswat**
  Visiting Faculty
  Department of Computer Science and Engineering
  Indian Institute of Technology Jammu
  India
  vishal.saraswat@iitjammu.ac.in
  Homepage: `http://www.crypta.in`
- **Dr. Sahadeo Padhye**
  Assistant Professor
  MNNIT Allahabad
  India
  sahadeomathrsu@gmail.com
  Homepage: `http://www.mnnit.ac.in/images/stories/sahadeo_CV_13-06-2014.pdf`