Biography of Dr. Abhijit Das

Introduction

Abhijit Das got his BE degree in Electronics and Telecommunication Engineering from Jadavpur University, Calcutta, in 1991, ME and PhD degrees from the Indian Institute of Science Bangalore in Computer Science and Engineering in 1993 and 2000, respectively. Dr. Das has spent a year in the Department of Mathematics, Ruhr-Universität Bochum, Germany as a Scientific Assistant, and a year as a Visiting Faculty member in the Department of Mathematics, Indian Institute of Technology Kanpur. Since 2002, he has been a permanent faculty member in the Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur. Currently, he is a Professor (since February 2018).

During his stay in IIT Kharagpur, Dr. Das has taught several courses in undergraduate and graduate levels. His academic and teaching interests are in the areas of algorithms, discrete mathematics, computational number theory, cryptography, formal languages and automata theory, complexity theory, graph theory, and parallel algorithms.

The main research interest of Dr. Das is computational number theory with applications to public-key cryptography and public-key cryptanalysis. He is also interested in efficient and parallel implementations of algorithms of interest in computational number theory and public-key cryptology. Some specific research areas of Dr. Das are algorithms for integer factorization and the discrete logarithm problem, elliptic-curve and pairing-based cryptography, cryptographic protocols in mobile and ad hoc networks, algebraic attacks, and massively parallel implementations of cryptographic and cryptanalytic algorithms. Dr. Das has more than 30 publications in refereed journals and conferences. He is the (co)author of two graduate-level textbooks on public-key cryptography and computational number theory.

Educational Qualifications

Degree	University/ Institution	Year	Discipline	Division/ Class	% of Marks	Rank in Board/University
PhD	Indian Institute of Science Bangalore	2000	Computer Science and Engineering	NA	NA	
ME	Indian Institute of Science Bangalore	1993	Computer Science and Engineering	First (Distinction)	7.7 (in 8)	
BE	Jadavpur University Calcutta	1991	Electronics and Tele-communication Engineering	First (Honours)	88.2%	
HS	WB Council for Higher Secondary Education	1987	Science	First	86.9%	Board Rank: 13th
Sec	WB Board for Secondary Education	1985	General	First	89.9%	Board Rank: 7th

Experience

University / Organization	Designation	From	To	Total Period	Nature of Experience
Indian Institute of Technology Kharagpur	Professor	Feb 2018	Present	–	Dept. of Computer Science & Engineering
Indian Institute of Technology Kharagpur	Associate Professor	May 2011	Feb 2018	6.5 Years	Dept. of Computer Science & Engineering
Indian Institute of Technology Kharagpur	Assistant Professor	Dec 2002	May 2011	8.5 Years	Dept. of Computer Science & Engineering
Indian Institute of Technology Kanpur	Visiting Faculty	Jan 2001	Dec 2001	1 Year	Dept. of Mathematics
Ruhr University, Bochum, Germany	Scientific Assistant	Oct 2000	Oct 2001	1 Year	Dept. of Mathematics
Indian Institute of Science, Bagalore	Project Associate	Jan 2000	Sep 2000	9 months	Funded by CDAC, Pune

Publications

Books

1. Abhijit Das, *Computational Number Theory*, Series: Discrete Mathematics and Its Applications, Chapman and Hall/CRC, ISBN: 9781439866153, March 18, 2013.

2. Abhijit Das and C. E. Veni Madhavan, *Public-key Cryptography: Theory and Practice*, Pearson Education, ISBN: 9788131708323, 2009.

3. Dipanwita Roy Chowdhury, Vincent Rijmen and Abhijit Das (Editors), *Progress in Cryptology—INDOCRYPT 2008*, 9th International Conference on Cryptology in India, Kharagpur, India, December 14–17, 2008. Proceedings, Lecture Notes in Computer Science #5365, Springer-Verlag, 2008.

Journal Papers

1. Binanda Sengupta and Abhijit Das, *Use of SIMD-based data parallelism to speed up sieving in integer-factoring algorithms*, Applied Mathematics and Computation, Volume 293, pp 204–217, Elsevier, January 2017.

2. Sabyasachi Karati, Abhijit Das, Dipanwita Roychowdhury, Bhargav Bellur, Debojyoti Bhattacharya and Aravind Iyer, *New algorithms for batch verification of standard ECDSA signatures*, Journal of Cryptographic Engineering, DOI: 10.1007/s13389-014-0082-x, Volume 4, Issue 4, pp 237–258, Springer-Verlag, November 2014 (online publication dated 26 July 2014).

3. Anup Kumar Bhattacharya, Sabyasachi Karati, Abhijit Das, Dipanwita Roychowdhury, Bhargav Bellur and Aravind Iyer, *Use of SIMD features to speed up eta pairing*, E-Business and Telecommunications, Communications in Computer and Information Science, DOI: 10.1007/978-3-662-44791-8_9, Volume 455, pp 137–154, Springer-Verlag, 2014.

4. Abhijit Das, Dipanwita Roychoudhury, Debojyoti Bhattacharya, Srinivasan Rajavelu, Rajeev Shorey and Tony Thomas, *Authentication schemes for VANETs: A survey*, International Journal of Vehicle Information and Communication Systems (IJVICS), Vol 3, No 1, pp 1–27, Inderscience Publishers, Jan 2013.

5. Anup Kumar Bhattacharya, Abhijit Das and Dipanwita Roychoudhury, *A simulation based framework to characterize pseudonymous authentication in VANET*, International Journal of Mobile and Adhoc Networks (IJMAN), Vol 1, Issue 1, May 2011.

6. Anshul Rai, Dipanwita Roychoudhury and Abhijit Das, *An efficient cross authentication protocol in VANET hierarchical model*, International Journal of Mobile and Adhoc Networks (IJMAN), Vol 1, Issue 1, May 2011.

7. Vivekananda Bhat K, Indranil Sengupta and Abhijit Das, *A new audio watermarking scheme based on singular value decomposition and quantization*, Circuits, Systems and Signal Processing, vol 30, pp 915–927, Springer-Verlag, Jan 2011.

8. Vivekananda Bhat K, Indranil Sengupta and Abhijit Das, *An audio watermarking scheme using singular value decomposition and dither-modulation quantization*, Journal of Multimedia Tools and Applications, DOI: 10.1007/s11042-010-0515-1, Volume 52, Issue 2–3, pp 369–383, Springer-Verlag, Apr 2011.

9. Vivekananda Bhat K, Indranil Sengupta and Abhijit Das, *An adaptive audio watermarking based on the singular value decomposition in the wavelet domain*, in Elsevier Journal of Digital Signal Processing, Volume 20, Issue 6, 1547–1558, December 2010.

10. Abhijit Das and C. E. Veni Madhavan, *On the Cubic Sieve Method for Computing Discrete Logarithms Over Prime Fields*, International Journal of Computer Mathematics (IJCM), 82(12), pp 1481–1495, 2005.

Conference Papers

1. Sabyasachi Karati and Abhijit Das, *Batch verification of EdDSA signatures*, 4th International Conference on Security, Privacy, and Applied Cryptography Engineering (SPACE 2014), Lecture Notes in Computer Science #8804, pp 256–271, Oct 18–22, 2014, Pune, India.

2. Sabyasachi Karati, Abhijit Das and Dipanwita Roychowdhury, *Randomized batch verification of standard ECDSA signatures*, 4th International Conference on Security, Privacy, and Applied Cryptography Engineering (SPACE 2014), Lecture Notes in Computer Science #8804, pp 237–255, Oct 18–22, 2014, Pune, India.

3. Sabyasachi Karati and Abhijit Das, *Faster Batch Verification of Standard ECDSA Signatures Using Summation Polynomials*, 12th International Conference on Applied Cryptography and Network Security (ACNS 2014), Lecture Notes in Computer Science #8479, pp 438–456, Jun 10–13, 2014, Lausanne, Switzerland.

4. Binanda Sengupta and Abhijit Das, *SIMD-Based Implementations of Sieving in Integer-Factoring Algorithms*, 3rd International Conference on Security, Privacy, and Applied Cryptography Engineering (SPACE 2013), Lecture Notes in Computer Science #8204, pp 40–55, Oct 19–23, 2013, Kharagpur, India.

5. Utsab Bose, Anup Kumar Bhattacharya and Abhijit Das, *GPU-based Implementation of 128-bit Secure Eta Pairing Over a Binary Field*, 6th International Conference on Cryptology in Africa (Africacrypt 2013), Lecture Notes in Computer Science #7918, pp 26–42, Jun 22–24, 2013, Cairo, Egypt.

6. Anup Kumar Bhattacharya, Abhijit Das, Dipanwita Roy Chowdhury, Arvind Iyer and Debojyoti Bhattacharya, *Autonomous certification with list-based revocation for secure V2V communication*, 8th International Conference on Information Systems Security (ICISS 2012), Lecture Notes in Computer Science #7671, pp 208–222, Dec 15–19, 2012, Guwahati, India.

7. Anup Kumar Bhattacharya, Abhijit Das, Dipanwita Roychowdhury, Bhargav Bellur and Aravind Iyer, *SIMD-based implementations of eta pairing over finite fields of small characteristics*, International Conference on Security and Cryptography (SECRYPT 2012), pp 94–101, Jul 24–27, 2012, Rome, Italy.

8. Satrajit Ghosh and Abhijit Das, *New variants of algebraic attacks based on structured Gaussian elimination* (extended abstract), Third International Conference on Symbolic Computation and Cryptography (SCC 2012), pp 119–125, Jul 10–13, 2012, Castro Urdiales, Spain.

9. Sabyasachi Karati, Abhijit Das, Dipanwita Roychowdhury, Bhargav Bellur, Debojyoti Bhattacharya and Aravind Iyer, *Batch verification of ECDSA signatures*, 5th International Conference on Cryptology in Africa (AfricaCrypt 2012), Lecture Notes in Computer Science #7374, pp 1–18, Jul 10–12, 2012, Ifrane, Morocco.

10. Arpan Mondal, Santosh Ghosh, Abhijit Das and Dipanwita Roychowdhury, *Efficient FPGA implementation of Montgomery multiplier using DSP blocks*, 16th International Symposium (VDAT 2012), Lecture Notes in Computer Science #7373, pp 370–372, Jul 1–4, 2012, Shibpur, India.

11. Santosh Ghosh, Dipanwita Roy Chowdhury and Abhijit Das, *High speed cryptoprocessor for eta pairing on 128-bit secure supersingular elliptic curves over characteristic two fields*, Workshop on Cryptographic Hardware and Embedded Systems 2011 (CHES 2011), Lecture Notes in Computer Science #6917, pp 442–458, Sep 28 – Oct 1, 2011, Nara, Japan.

12. Satrajit Ghosh and Abhijit Das, *An improvement of linearization-based algebraic attacks*, International Conference on Security Aspects in Information Technology, High-Performance Computing and Networking (InfoSecHiComNet 2011), in Lecture Notes in Computer Science #7011, pp 157–167, Oct 19–22, 2011, Haldia.

13. Souvik Bhattacherjee and Abhijit Das, *Parallelization of the Lanczos Algorithm on Multi-core Platforms*, 11th International Conference on Distributed Computing and Networking (ICDCN 2010), in Lecture Notes in Computer Science #5935, pp 231–241, Jan 3–6, 2010, Calcutta.

14. Vivekananda Bhat K, Indranil Sengupta and Abhijit Das, *Audio Watermarking Based on BCH Coding Using CT and DWT*, 11th International Conference on Information Technology (ICIT 2008), IEEE Computer Society, pp 49–50, Dec 17–20, 2008, Bhubaneshwar.

15. Vivekananda Bhat K, Indranil Sengupta and Abhijit Das, *Audio Watermarking Based on Quantization in Wavelet Domain*, 4th International Conference on Information Systems Security (ICISS 2008), in Lecture Notes in Computer Science #5352, pp 235–242, Dec 16–20, 2008, Hyderabad.

16. Vivekananda Bhat K, Indranil Sengupta and Abhijit Das, *Audio Watermarking Based on Mean Quantization in Cepstrum Domain*, 16th International Conference on Advanced Computing and Communication (ADCOM 2008), Dec 14–17, 2008, Chennai.

17. Abhijit Das and Bimal Kumar Roy, *A New Key-Predistribution Scheme for Highly Mobile Sensor Networks*. 9th International Conference on Distributed Computing and Networking (ICDCN 2008), Lecture Notes in Computer Science, #4904, pp 298–303, Jan 5–8, 2008, Kolkata.

18. Ashok Kumar Das, Abhijit Das, Surjyakanta Mahapatra and Srihari Vavilapalli, *A Location-Aware Scheme for Key Establishment in Wireless Sensor Networks*, 1st International Conference on Communication System Software and Middleware, 2006 (COMSWARE 2006), IEEE Computer Society, pp 1–5, January 2006, New Delhi.

19. Ashok Kumar Das, Abhijit Das, Surjyakanta Mohapatra and Srihari Vavilapalli, *Key Forwarding: A Location-Adaptive Key-Establishment Scheme for Wireless Sensor Networks*, 7th International Workshop on Distributed Computing (IWDC 2005), Lecture Notes in Computer Science, #3741, pp 404–409, Dec 27–30, 2005, Kharagpur.

20. Abhijit Das and C E Veni Madhavan, *Performance Comparison of Linear Sieve and Cubic Sieve Algorithms for Discrete Logarithms over Prime Fields*, 10th International Symposium on Algorithms and Computation (ISAAC 1999), Lecture Notes in Computer Science, #1741, pp 295–306, Dec 16–18, 1999, Chennai.

21. Abhijit Das, *Bengali Writer Utilities*, Information Revolution and Indian Languages (IRIL), pp 13.1–13.6, Nov 1999, Hyderabad.

22. Abhijit Das, Abhik Mukherjee and Amit Konar, *An Expert System for Decision Making in Nonmonotonic Domain*, International Conference on Energy, Computer, Communication and Control Systems, IEEE, Vol 3, pp 269–272, Aug 1991.

Theses

- **PhD Thesis:** *Galois Field computations: Implementation of a library and a study of the discrete logarithm problem*, Faculty of Engineering, Indian Institute of Science, Sep 1999.

- **ME Thesis:** *Load balancing on an extended hypercube*, Indian Institute of Science, Jan 1993.

Google Scholar Records (As on 27-Jun-2019)

Number of articles: 36
Number of citations: 579
H-index: 11
I10-index: 11

Research Guidance

PhD students

7. Debranjan Pal
   Area: Cryptography and security
   Co-supervisor: Dipanwita Roy Chowdhury
   Joined in: July 2018

6. Bijoy Das
   Area: Security and privacy
   Co-supervisor: Dipanwita Roy Chowdhury
   Joined in: July 2017

5. Souvik Sur
   Area: Crypto-currencies
   Co-supervisor: Dipanwita Roy Chowdhury
   Joined in: July 2016

4. Sabyasachi Karati
   Thesis title: *Batch verification of elliptic curve and Edwards curve digital signatures*
   Co-supervisor: None
   Date: 2015

3. Vivekananda Bhat K
   Thesis title: *Digital watermarking of audio signals using quantization*
   Co-supervisor: Indranil Sen Gupta
   Date: 2010

2. Ashok Kumar Das
   Thesis title: *Design and analysis of key distribution mechanisms in wireless sensor networks*
   Co-supervisor: Indranil Sen Gupta
   Date: 2008

1. Debasis Giri
   Thesis title: *Cryptanalysis and improvement of protocols for digital signature, smart-card authentication and access control*
   Co-supervisor: P D Srivastava
   Date: 2008

MS students

9. Md Rasid Ali
   Area: Symmetric cryptology
   Co-supervisor: Dipanwita Roy Chowdhury
   Joined in: January 2019

8. Shramona Chakraborty
   Area: Symmetric cryptology
   Co-supervisor: Dipanwita Roy Chowdhury
   Joined in: January 2019

7. Rahul Roy
   Area: Integer factorization
   Co-supervisor: Dipanwita Roy Chowdhury
   Joined in: January 2019

6. Pritam Pallab
   Area: Integer factorization
   Co-supervisor: None
   Joined in: January 2018

5. Anindya Ganguly
   Area: Hyperelliptic-curve cryptography
   Co-supervisor: Dipanwita Roy Chowdhury
   Joined in: January 2017

4. Binanda Sengupta
   Thesis title: *SIMD-based implementations of sieving in integer-factoring algorithms*
   Co-supervisor: None
   Date: 2013

3. Satrajit Ghosh
   Thesis title: *Improvements of linearization-based algebraic attacks on block ciphers*
   Co-supervisor: None
   Date 2012

2. Anup Kumar Bhattacharya
   Thesis title: *Efficient software implementation of elliptic-curve pairing*
   Co-supervisor: Dipanwita Roy Chowdhury
   Date: 2011

1. Souvik Bhattacherjee
   Thesis title: *Parallel and distributed implementations of the Lanczos sparse system solver over large prime fields*
   Co-supervisor: None
   Date: 2011

Projects

No	Name	Sponsor	Role	Status
1	Investigation of Cryptanalytic Techniques (ICT)	Headquarters, Integrated Defence Staff, Ministry of Defence, Government of India	Principal investigator	Completed
2	Design and Analysis of an Efficient Cryptosystem for Safety Messaging over Vehicular Networks (CRLP)	General Motors (R&D), India	Co-principal investigator	Completed
3	Design and Efficient Implementation of Advanced Encryption and Decryption Techniques for Use in Spacecraft Communication (EEC)	ISRO, IIT Kharagpur Cell, Space Technology Cell, India	Principal investigator	Nearing completion
4	Cryptanalysis of Cryptographic Ciphers with Emphasis on AES and RSA (CER)	Ministry of Electronics and Information Technology, Government of India	Co-principal investigator	In progress

Top Teaching Feedback

Course	Semester	Level	Institute Rank
Algorithms Laboratory	Spring 18–19	UG	4 in Lab (50+), 2 in Lab (100+) categories
Computing Lab – I	Autumn 18–19	PG	4 in Lab (25+), 1 in Lab (50+) categories
Algorithms Laboratory	Spring 17–18	UG	3 in Lab (50+), 2 in Lab (100+) categories
Algorithms Laboratory	Autumn 17–18	UG	3 in Lab (100+) category
Algorithms Laboratory	Autumn 16–17	UG	2 in Lab (50+) and (100+) categories
Switching Circuits and Logic Design	Spring 15–16	UG	1 in Theory (100+) category
Switching Circuits Laboratory	Spring 15–16	UG	2 in Lab (50+) and (100+) categories
Algorithms Laboratory	Autumn 15–16	UG	2 in Lab (50+ and 100+) categories
Algorithms Laboratory	Autumn 14–15	UG	3 in Lab (50+ and 100+) categories

Academic and Professional Awards

- University medal, Jadavpur University, 1991
- T P Saha Gold-Centered medal, Jadavpur University, 1991
- CSI (Bangalore) medal, Indian Institute of Science, 1993
- Motorola medal, Indian Institute of Science, 1993