+91-8056267430
gautham.sekar@gmail.com, gautham@mse.ac.in

GAUTHAM SEKAR

INTERESTS

Cryptology & Information Security
Data Science & Analytics
Financial Technology
Philosophy

EMPLOYMENT

ASSISTANT PROFESSOR, MADRAS SCHOOL OF ECONOMICS, INDIA

May 2022 to Present

Post Graduate Diploma in Management (PGDM) Chair

Courses:
Mathematical Statistics (MA-AQF): Currently co-teaching
Statistics for Economics (BA Batch 1): Currently teaching
Probability (PGDM Batch 6): Currently teaching
Research and Publication Ethics (PhD): Co-taught
Mathematical Methods for Economics II (BA Batch 1): Covered Linear Algebra
Information Theory and Cryptography (PGDM Batch 4): Students' feedback rating of 4.84/5 (average of 20 ratings, each involving 18 parameters).
Advanced Analytical Models for Decision Making (PGDM Batch 4): Students' feedback rating of 4.59/5 (average of 20 ratings, each involving 18 parameters).
Statistical Inference and Modeling (PGDM Batch 5): Students' feedback rating of 4.62/5 (average of 21 ratings, each involving 18 parameters).
Probability (PGDM Batch 5): Students' feedback rating of 4.28/5 (average of 23 ratings, each involving 18 parameters).

FOUNDER & PRESIDENT, MADRAS FINTECH SERVICES PVT. LTD, INDIA

December 2019 to Present

Founded the company with an aim to provide innovative services to the finance, information & communication technology (ICT) and education sectors. The services include research, development of software & methodologies, designing of algorithms, financial & technological advising, and corporate training. The company is a Member of the **Information Systems Security and Privacy Committee** (LITD 17 / Panel 6) of the **Bureau of Indian Standards**. Our past clients include Infineon Technologies AG (Germany) and National Power Training Institute (India).

VISITING FACULTY, MADRAS SCHOOL OF ECONOMICS, INDIA

August-November 2020, February-June 2021, February-May 2022

Taught **Cryptography** for PGDM. Students' feedback rating: 4.40/5 (average of 9 ratings, each involving 18 parameters).

Taught **Information Theory and Cryptography** for PGDM. Students' feedback rating: 4.25/5 (average of 24 ratings, each involving 18 parameters).

Co-taught **Advanced Analytical Models for Decision Making** for PGDM. Students' feedback rating: 4.50/5 (average of 15 ratings, each involving 18 parameters).

GUEST FACULTY, BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE (BITS) PILANI, INDIA

October 2019 to January 2021

- Taught **Probability & Statistics** for HCL TechBee (Job Programme).
  Students' feedback rating: 4.58/5 (average of 31 ratings).
- Taught **Introduction to Statistical Methods** for Off-Campus M.Tech. Data Science & Engineering.

VISITING FELLOW, RAMANUJAN INSTITUTE OF ADVANCED STUDY IN MATHEMATICS, INDIA

December 2019 to March 2020

Taught **Probability Theory** for M.Sc. Mathematics.

ASSISTANT PROFESSOR, CR RAO AIMSCS, INDIA

April-September 2018

VISITING FACULTY, THE INSTITUTE OF MATHEMATICAL SCIENCES, INDIA

January 2016 to June 2017

VISITING ASSISTANT PROFESSOR, INDIAN STATISTICAL INSTITUTE, INDIA

May 2012 to November 2015

- Co-taught **Programming & Data Structures** for M.Stat.
- Co-taught **Probability & Stochastic Processes II** for M.Stat (Applications).

RESEARCH SCIENTIST, NATIONAL UNIVERSITY OF SINGAPORE, SINGAPORE

April 2011 to March 2012

EDUCATION

DOCTOR OF ENGINEERING (CRYPTOGRAPHY) – KU LEUVEN – BELGIUM – 2011

Advisor: Prof. Dr Bart Preneel

MASTER OF SCIENCE (HONOURS) IN PHYSICS – BITS PILANI – INDIA – 2006

Thesis Advisor: Prof. Dr Bart Preneel

BACHELOR OF ENGINEERING (HONOURS) IN ELECTRONICS & INSTRUMENTATION – BITS PILANI – INDIA – 2006

Project Advisors: Prof. Dr R. Balasubramanian (IMSc) and Prof. Dr Srinivas Kotyada (IMSc)

PEER-REVIEWED PUBLICATIONS

(SCOPUS / AMS INDEXED)

1. Mabin Joseph, **Gautham Sekar**, R. Balasubramanian, **Revisiting the Software-Efficient Stream Ciphers RCR-64 and RCR-32**. The Computer Journal, published 14 August 2023. DOI: https://doi.org/10.1093/comjnl/bxad084.

2. Mabin Joseph, **Gautham Sekar**, R. Balasubramanian, G. Venkiteswaran, **On the Security of the Stream Ciphers RCR–64 and RCR–32**, The Computer Journal, vol. 65(12), pp. 3091–3099, 2022.

3. Mabin Joseph, **Gautham Sekar**, R. Balasubramanian, **Side Channel Analysis of SPECK**, Journal of Computer Security, vol. 28(6), pp. 655–676, 2020.

4. **Gautham Sekar**, Soumyadeep Bhattacharya, **Practical (Second) Preimage Attacks on the TCS_SHA-3 Family of Cryptographic Hash Functions**, Journal of Information Processing Systems, vol. 12(2), pp. 310–321, 2016.

5. Mabin Joseph, **Gautham Sekar**, Balasubramanian Ramachandran, **Distinguishing Attacks on (Ultra-)lightweight WG Ciphers**, LightSec 2016 (A. Bogdanov, ed.), vol. 10098 of LNCS, pp. 45–59. Springer, 2017.

6. **Gautham Sekar**, **Side Channel Cryptanalysis of Streebog**, SSR – Security Standardisation Research 2015 (L. Chen, S. Matsuo, eds.), vol. 9497 of LNCS, pp. 154–162. Springer, 2015. **(Preliminary version presented as a short paper at CTCrypt 2015.)**

7. **Gautham Sekar**, Nicky Mouha, Bart Preneel, **Meet-in-the-middle attacks on reduced-round GOST**, Mathematical Aspects of Cryptography, vol. 5(2), pp. 117–125, 2014.

8. Nicky Mouha, **Gautham Sekar**, Bart Preneel **Challenging the increased resistance of regular hash functions against birthday attacks**, Journal of Mathematical Cryptology, vol. 6(3–4), pp. 229–248, 2012.

9. **Gautham Sekar**, **The Stream Cipher Core of the 3GPP Encryption Standard 128-EEA3: Timing Attacks and Countermeasures**, Inscrypt 2011 (C. Wu, M. Yung, D. Lin, eds.), vol. 7537 of LNCS, pp. 269–288. Springer, 2012.

10. **Gautham Sekar**, Bart Preneel, **Practical Attacks on a Cryptosystem Proposed in Patent WO/2009/066313**, WISA –Workshop on Information Security Applications 2011 (S. Jung, M. Yung, eds.), vol. 7115 of LNCS, pp. 1–12. Springer, 2012.
(Received the highest review score.)

11. **Gautham Sekar**, Nicky Mouha, Vesselin Velichkov, Bart Preneel, **Meet-in-the-Middle Attacks on Reduced-Round XTEA**, CT-RSA – The Cryptographers' Track at the RSA Conference 2011 (A. Kiayias, ed.), vol. 6558 of LNCS, pp. 250–267. Springer, 2011.

12. Nicky Mouha, **Gautham Sekar**, Jean-Philippe Aumasson, Thomas Peyrin, Søren S. Thomsen, Meltem Sönmez Turan, Bart Preneel, **Cryptanalysis of the ESSENCE Family of Hash Functions**, Inscrypt 2009 (F. Bao, M. Yung, D. Lin, J. Jing, eds.), vol. 6151 of LNCS, pp. 15–34. Springer, 2010.

13. **Gautham Sekar**, Bart Preneel, **Improved Distinguishing Attacks on HC-256**, IWSEC – International Workshop on Security 2009 (T. Takagi, M. Mambo, eds.), vol. 5824 of LNCS, pp. 38–52. Springer, 2009.

14. Jorge Nakahara Jr., **Gautham Sekar**, Daniel Santana de Freitas, Chang Chiann, Ramon Hugo de Souza, Bart Preneel, **A New Approach to $\chi 2$ Cryptanalysis of Block Ciphers**, ISC – Information Security Conference 2009 (P. Samarati, M. Yung, F. Martinelli, C. A. Ardagna, eds.), vol. 5735 of LNCS, pp. 1–16. Springer, 2009.

15. Emilia Käsper, Vincent Rijmen, Tor E. Bjørstad, Christian Rechberger, Matthew J. B. Robshaw, **Gautham Sekar**, **Correlated Keystreams in Moustique**, AFRICACRYPT 2008 (S. Vaudenay, ed.), vol. 5023 of LNCS, pp. 246–257. Springer, 2008.

16. Orr Dunkelman, **Gautham Sekar**, Bart Preneel, **Improved Meet-in-the-Middle Attacks on Reduced-Round DES**, INDOCRYPT 2007 (K. Srinathan, C. Pandu Rangan, M. Yung, eds.), vol. 4859 of LNCS, pp. 86–100. Springer, 2007.

17. **Gautham Sekar**, Souradyuti Paul, Bart Preneel, **Related-Key Attacks on the Py-Family of Ciphers and an Approach to Repair the Weaknesses**, INDOCRYPT 2007 (K. Srinathan, C. Pandu Rangan, M. Yung, eds.), vol. 4859 of LNCS, pp. 58–72. Springer, 2007.

18. **Gautham Sekar**, Souradyuti Paul, Bart Preneel, **New Weaknesses in the Keystream Generation Algorithms of the Stream Ciphers TPy and Py**, ISC – Information Security Conference 2007 (J. A. Garay, A. K. Lenstra, M. Mambo, R. Peralta, eds.), vol. 4779 of LNCS, pp. 249–262. Springer, 2007.

19. **Gautham Sekar**, Souradyuti Paul, Bart Preneel, **New Attacks on the Stream Cipher TPy6 and Design of New Ciphers the TPy6-A and the TPy6-B**, WEWoRC – Western European Workshop on Research in Cryptology 2007 (S. Lucks, A.-R. Sadeghi, C. Wolf, eds.), vol. 4945 of LNCS, pp. 127–141. Springer, 2008.

20. Souradyuti Paul, Bart Preneel, **Gautham Sekar**, **Distinguishing Attacks on the Stream Cipher Py**, FSE – Fast Software Encryption 2006 (M. J. B. Robshaw, ed.), vol. 4047 of LNCS, pp. 405–421. Springer, 2006.

JOURNAL SUBMISSIONS IN REVIEW

1. **Gautham Sekar**, Ardra K.M., Himanshu Shekhar, Sudharshan T.R., Srirangapriya G., Reya Jessica, Rakesh Nigam, **Analysis of HIGHT and Functional Meet-in-the-Middle Attacks**. Status: Past the Rebuttal stage.

2. Mabin Joseph, **Gautham Sekar**, R. Balasubramanian, **Fault-Assisted Side Channel Analysis of HMAC-Streebog**.
(Also presented as a paper at CTCrypt 2020.)

DELIVERABLES

1. Andrey Bodganov, Nicky Mouha, **Gautham Sekar**, Elmar Tischhauser, Deniz Toz, Kerem Varici, Vesselin Velichkov, Meiqin Wang, **Security Evaluation of the K2 Stream Cipher**, CRYPTREC deliverable (A. Bodganov, B. Preneel, V. Rijmen, eds.), 7 March 2011.

2. Tor E. Bjørstad, Andrey Bogdanov, Henri Gilbert, Kota Ideguchi, Sebastiaan Indesteege, Özgül Küçük, Gregor Leander, Nicky Mouha, Jorge Nakahara Jr., Axel Poschmann, Christian Rechberger, Vincent Rijmen, **Gautham Sekar**, Kyoji Shibutani, Martin Schläffer, François-Xavier Standaert, Elmar Tischhauser, Vesselin Velichkov, Ivan Visconti, **WG2 – Lightweight Cryptographic Algorithms**, D.SYM.5, ICT-2007-216676, ECRYPT II deliverable (J. Nakahara Jr., ed.), delivered 1 July 2010.

REVIEW WORK

Member of Programme Committee, Security Standardisation Research (SSR) 2015, Tokyo, Japan, December 15–16, 2015

Former Member of Editorial Board, Journal of Information Processing Systems

Reviewed for the Computer Journal, IEEE Transactions on Information Forensics and Security, Information Sciences, Security and Communication Networks, IET Information Security, Fast Software Encryption, ASIACRYPT, Information Security Conference, Cryptographers Track – RSA Conference, etc.

DOCTORAL GUIDANCE

Technology Advisor, Mabin Joseph, Indira Gandhi Centre for Atomic Research (IGCAR), Kalpakkam, India. Date of PhD defence: 23 May 2023.

TALKS

1. “Improved Chebyshev Bound Under Restriction”, MSE Faculty Seminar, Madras School of Economics, India, 3 March 2023.

2. “Cyber Security Best Practices”, Cyber Security Issues & Challenges in Smart Power Systems, National Power Training Institute, Neyveli, India, Webinar, 21 April 2022. (Invited)

3. “Cryptography and Key Management”, Cyber Security Issues & Challenges in Smart Power Systems, National Power Training Institute, Neyveli, India, Webinar, 21 April 2022. (Invited)

4. “Information Security Practices”, Data Science and Security Primer, Education & Research Network India, Webinar, 18 August 2021. (Invited)

5. “Information Security and Data Science”, ATAL Faculty Development Programme on Data Sciences, National Power Training Institute, Neyveli, India, Webinar, 13 August 2021. (Invited)

6. “Using Decision Trees in Decision Making”, National Productivity Council of India, Webinar, 30 September 2020. (Guest Lecture)

7. “Fundamentals of Decision Theory”, National Productivity Council of India, Webinar, 16 September 2020. (Guest Lecture)

8. “Revisiting Shannon’s Theory of Cryptology”, XXII Ramanujan Symposium: National Conference on Pure and Applied Mathematics, Chennai, India, 8 March 2019. (Invited)

9. “Algorithmic Cryptanalysis and Implementation Attacks: Case Studies with Russian Standards”, Indian Institute of Technology Palakkad, India, 8 October 2018. (Invited)

10. “Some Recent Results on Russian Cryptographic Standards”, The Institute of Mathematical Sciences, Chennai, India, 27 November 2015. (Invited)

11. “Meet-in-the-Middle Attacks on Reduced-Round GOST”, Tata Consultancy Services, Hyderabad, India, 27 March 2015. (Invited)

12. “Areal Data Analysis”, National Level Workshop on Developments in Statistical Methods for Data Analysis of Excluded Groups, Mysore, India, 20 March 2014. (Invited)

13. “Statistical Timing Analysis: the Case of the LTE Standard 128-EEA3”, National Workshop on Cryptology 2012, Vellore, India, 8 August 2012. (Invited)

14. “Cryptanalysis of the ESSENCE Family of Hash Functions”, Institute of Mathematics and Applications, Bhubaneswar, India, 12 January 2010. (Invited)

15. “The Py-Family of Stream Ciphers”, Institute of Mathematics and Applications, Bhubaneswar, India, 6 December 2008. (Invited)

16. Contributed talks at reputed conferences and workshops in India, Russia, China, South Korea, Japan, Austria, Chile and Germany.

17. Institute student seminars in India and Belgium.

MEMBERSHIPS

Cryptology Research Society of India (Life Member)

International Association for Cryptologic Research (2007, 2010)

AWARDS & HONOURS

1. Recognised as a "**valued member of the ISO technical committee**" and an "**active contributor to ISO work from India**". Invited to the **ISO Annual Meeting** in September 2023.

2. Part of the **Indian delegation for ISO/IEC JTC 1/SC 27** "Information security, cybersecurity and privacy protection" meetings in 2022 and 2023.

3. A secure implementation of a 3GPP encryption standard that I co-developed is included in the **LTE wireless standards**.

4. Received **Katholieke Universiteit Leuven Scholarship** for (pre-)doctoral studies (Nov. 2006 – Mar. 2011) and master's thesis (Aug. 2005 – Jan. 2006).

5. Received **Dr. Ranjit Singh Chauhan Undergraduate Research Award** from BITS Pilani in May 2007. (Was the sole recipient for the year from among thousands of students.)

6. Selected as an **Undergraduate Associate of the Saha Institute of Nuclear Physics**, Kolkata, India (2002).

7. Qualified the **Regional Mathematical Olympiad** for Tamil Nadu and Pondicherry, India (1999).

MISCELLANEOUS

1. Mentored interns from reputed universities including Indian Institutes of Technology, National Institute of Technology and BITS Pilani.

2. Co-organised tutorials and workshops at the Indian Statistical Institute, Institute of Mathematics and Applications (Bhubaneswar, India) and the Institute of Mathematical Sciences (Chennai, India).

3. Contributed to open international projects such as ECRYPT (Europe), CRYPTREC (Japan) and NIST SHA-3 (USA).

4. Nationality: Indian

5. Date of birth: 14 August 1984

REFEREES

Available on request.

DECLARATION

The information furnished by me in this CV is true to the best of my knowledge and belief.

(CV last updated October 2023)