

Research

- Information Security
- Blockchain Technology

Programming

- Java
- Javascript
- C and C++
- nesC (TinyOS)

Award

Won the cash prize and citation at the fifth IDRBT doctoral colloquium, Hyderabad, India (Dec-2015).

Contact



www.keyurparmar.in
www.linkedin.com/in/keyur-parmar/

Education

- **Doctor of Philosophy - Computer Engineering**
“Secure In-network Processing of Encrypted Data in Wireless Sensor Networks”
S. V. National Institute of Technology, Surat, India, 2016.
- **Master of Technology - Computer Engineering** [First Class with Distinction]
“Novel Approaches for Verifiable Secret Sharing”
S. V. National Institute of Technology, Surat, India, 2010.
- **Bachelor of Engineering - Information Technology** [First Class]
V. Government Engineering College (Gujarat University), Gandhinagar, India, 2007.

Experience

- **Assistant Professor**
Indian Institute of Information Technology (IIIT), Vadodara, India.
Duration: 2016 - Present
- **Senior Research Fellow**
S. V. National Institute of Technology, Surat, India.
Duration: 2011 - 2015
- **Project Scientist**
B. Institute for Space Applications and Geo-Informatics, Gandhinagar, India.
Year: 2011

Publications

Book Chapter

- [1] **Malleable Cryptosystems and Their Applications in Wireless Sensor Networks**
Keyur Parmar and Devesh C. Jinwala
Computer and Network Security Essentials, Springer-Verlag, pp. 97–111, 2018, DOI: 10.1007/978-3-319-58424-9_6.

Journals

- [1] **Concealed Data Aggregation in Wireless Sensor Networks: A Comprehensive Survey**
Keyur Parmar and Devesh C. Jinwala
Computer Networks, Elsevier, 103 (7), pp. 207–227, 2016, DOI: 10.1016/j.comnet.2016.04.013.
- [2] **Malleability Resilient Concealed Data Aggregation in Wireless Sensor Networks**
Keyur Parmar and Devesh C. Jinwala
Wireless Personal Communications, Springer-Verlag, 87 (3), pp. 971–993, 2016, DOI: 10.1007/s11277-015-2633-6.

- [3] **Symmetric-Key Based Homomorphic Primitives for End-to-End Secure Data Aggregation in Wireless Sensor Networks**
Keyur Parmar and Devesh C. Jinwala
Journal of Information Security, Scientific Research, 6 (1), pp. 38–50, 2015, DOI: 10.4236/jis.2015.61005.

International Conferences/Workshops

- [1] **Hybrid Secure Data Aggregation in Wireless Sensor Networks**
Keyur Parmar and Devesh C. Jinwala
Proceedings of the 5th Workshop on Design, Modeling and Evaluation of Cyber Physical Systems, CyPhy, Vol. 9361 of Lecture Notes in Computer Science, Springer-Verlag, Amsterdam, The Netherlands, pp. 116–131, 2015, DOI: 10.1007/978-3-319-25141-7_9.
- [2] **End-to-End Secure Data Aggregation in Wireless Sensor Networks**
Keyur Parmar and Devesh C. Jinwala
Doctoral Symposium of the 10th International Conference on Information Systems Security, ICISS of Hyderabad, India, pp. 1–4, 2014.
- [3] **Malleability Resilient Concealed Data Aggregation**
Keyur Parmar and Devesh C. Jinwala
Proceedings of the 20th EUNICE/IFIP WG 6.2, 6.6 Workshop on Advances in Communication Networking, EUNICE, Vol. 8846 of Lecture Notes in Computer Science, Springer-Verlag, Rennes, France, pp. 160–172, 2014, DOI: 10.1007/978-3-319-13488-8_15.
- [4] **Aggregate MAC Based Authentication for Secure Data Aggregation in Wireless Sensor Networks**
Keyur Parmar and Devesh C. Jinwala
Proceedings of the 10th International Conference on Intelligent Computing, ICIC, Vol. 8589 of Lecture Notes in Artificial Intelligence, Springer-Verlag, Taiyuan, China, pp. 475–483, 2014, DOI: 10.1007/978-3-319-09339-0_48.

National Conferences/Workshops

- [1] **Secure In-network Processing of Encrypted Data in Wireless Sensor Networks**
Keyur Parmar and Devesh C. Jinwala
The 5th IDRBT Doctoral Colloquium, Hyderabad, India, pp. 1–6, 2015.
- [2] **A Novel Approach for Verifiable Secret Sharing Using a One Way Hash Function**
Keyur Parmar and Devesh C. Jinwala
Proceedings of the 10th National Workshop on Cryptology, PSG College of Technology, Coimbatore, India, pp. 18–23, 2010.

Invited Talks

- **Security Issues in Resource-constrained WSNs**
Sarvajani College of Engineering & Technology (Department of Information Technology), Surat, India, 2017.
- **Broadcast/Convergecast Authentication in Wireless Sensor Networks**
A Short Term Training Programme (STTP) on Wireless Sensor Networks: Secure Data Aggregation and Related Issues (WSN-SDARI)
S. V. National Institute of Technology, Surat, India, 2014.

- **Broadcast Authentication in Wireless Sensor Networks**
A Short Term Training Programme (STTP) on Wireless Sensor Networks & Security Issues
S. V. National Institute of Technology, Surat, India, 2013.
- **Number Theoretic Problems and Their Applications in Cryptography**
A Short Term Training Programme (STTP) on Wireless Sensor Networks: Secure Data Aggregation and Related Issues (WSN-SDARI)
S. V. National Institute of Technology, Surat, India, 2013.
- **Broadcast Authentication in Wireless Sensor Networks**
A Short Term Training Programme (STTP) on Wireless Sensor Networks: Secure Data Aggregation and Related Issues (WSN-SDARI)
S. V. National Institute of Technology, Surat, India, 2013.

Professional Activities

- **Memberships**
 - International Association for Cryptologic Research (IACR) [Member ID: 20180529]
 - Association for Computing Machinery (ACM) [Member ID: 7887878]
 - Institute of Electrical and Electronics Engineers (IEEE) [Member ID: 93125135]
 - Cryptology Research Society of India (CRSI) [Member ID: L/0469]
 - Indian Society For Technical Education (ISTE) [Member ID: LM 77337]
 - **Reviewer, Sub-Reviewer or Technical Program Committee Member**
 - **Journals:** Transactions on Dependable and Secure Computing (IEEE, 2018), Transactions on Industrial Informatics (IEEE, 2017), Wireless Personal Communications (Springer, 2014-2015), Transactions on Internet and Information Systems (KSII, 2015-2018), Cryptography and Communications (Springer, 2012), etc.
 - **Conferences/Workshops:** ISEA-ISAP (Springer-Verlag, Jaipur, India, 2018), ICISS (Springer-Verlag, Jaipur, India, 2016), TENCON (IEEE, Marina Bay Sands, Singapore, 2016), ICCCT (IEEE, Allahabad, India, 2014), ICDCIT (Springer-Verlag, Bhubaneswar, India, 2014), etc.
 - **Session Chair, Coordinator or Organizer**
 - SPIoE'19: Security and Privacy Issues in the Internet of Everything, ICDCN, Indian Institute of Science, Bangalore, India, Session Chair, 2019.
 - Latex Workshop, BISAG, Gandhinagar & IIT, Bombay, India, Coordinator, 2011.
-