M B S Venkatesh

☎ (+91) 7506134390
✉ bhargav.eecs@gmail.com
bhargav-svm.github.io

Education

2013–2017 **Bachelor of Technology (Honors)**, *Electrical Engineering*.
Indian Institute of Technology Bombay (IIT-B)
Minors in Computer Science and Engineering
CGPA - 8.81/10.0

Interests

Applied Cryptography, Cryptanalysis, Learning Algorithms

Research Contributions

Design, Implementation and Performance Analysis of Highly efficient Algorithms for AES key Retrieval in Access-driven Cache-based Side Channel Attacks, C Ashokkumar, **MBS Venkatesh**, RP Giri, B Menezes, Technical Report, CSE, IIT Bombay, 2016

An error-tolerant approach for efficient AES key retrieval in the presence of cache prefetching - Experiments, Results, Analysis, C Ashokkumar, **MBS Venkatesh**, RP Giri, B Roy, B Menezes, accepted by Sadhana, Official Journal of the Indian Academy of Sciences, 2018.

"S-Box" Implementation of AES is NOT side-channel resistant, C Ashokkumar, B Roy, **MBS Venkatesh**, B Menezes, 2018 (under review)

Cryptanalysis of Galbraith's Binary LWE, T Sanyashi, **MBS Venkatesh**, B Menezes, 2018 (to be submitted)

Scholastic Achievements

- All India Rank 336 in the Joint Entrance Exam (JEE) Advanced 2013, amongst 1.4 million examinees (**top 0.025% percentile**).
- Received an **AP grade** for exceptional performance in a course on Linear Algebra.
- **KVPY** fellowship from Government of India in 2011.
- **All India Rank 9** in National level Mathematics Test by AMTI, India in 2012.
- **Gold Medal** and INTEL Award of Excellence for overall best performance at IGNOU-UNESCO Science Olympiad conducted among SAARC countries in 2011.
- Among top **1%** (300) students in India in Mathematics, Physics and Astronomy National Olympiads in 2011 and 2012

Key Academic and Research Projects

Ongoing **Cryptanalysis of Binary LWE Cryptosystem**.

Mentor: *Prof. Bernard Menezes*, IIT-B.

- Trying to break Galbraith's Binary LWE based cryptosystem using solvers of Linear Programming (LP) and Closest Vector Problem (CVP).
- Designed a strategy to increase success rate to 15% (previous best is 1%).

2015-17 **AES Key Retrieval in Cache-based Side Channel Attacks**.

Mentor: *Prof. Bernard Menezes*, IIT-B.

- Designed algorithms to deduce the AES key in both known-ciphertext attack and known-plaintext attack using the set of accessed (ambiguous) cache line numbers.
- Developed probability models to predict the optimal parameters for the designed algorithms and to quantify their performance.
- Successfully attacked multiple software impentations of AES including the assembly version using less than 50 blocks and retrieved secret key almost always.

2016-17 **A Case Study of Remote Voting Systems**.

Mentor: *Prof. R.K.Shyamasundar*, IIT-B.

- Studied Civitas, a remote voting system extensively and analysed the protocols involved in every step of the system. We verified that Civitas ensures Voter's ability to resist coercion, Privacy of the voter and Universal verifiability.
- Based on our analysis of Civitas and other voting systems, we have listed out drawbacks in current voting scenarios and suggested ways to overcome some of them.

Spring'17 **Oblivious Transfer and Garbled Circuits**.

Mentor: *Prof. Manoj Prabhakaran*, IIT-B.

- Studied Oblivious transfer protocols for semi-honest and malicious adversary models.
- Analysed Yao's garbled circuits protocol and other efficient variants of it.

Spring'17 **DSA Signing Key Recovery in Side Channel Attacks**.

Mentor: *Prof. Bernard Menezes*, IIT-B.

- Studied cache based side-channel attacks on DSA and ECDSA to obtain partial information of ephemeral keys. Reviewed literature on hard lattice problems, their solvers and their use in retrieving the complete secret key with partial information from side-channel.

Fall'16 **Intelligent Carrom Playing Agent**.

Mentor: *Prof. Shivaram Kalyankrishnan*, IIT-B.

- Developed an agent to play the carroms game using Q-Learning technique.
- Due to continuous state and action space, we trained a neural network to predict Q-values.

Summer'16 **Object Detection and Face Recognition**.

Mentor: *Prof. Ganesh Ramakrishnan*, IIT-B.

- Implemented a Object Detection system using Convolutional Neural Networks.
- Developed a Face Recognition system from scratch based on Principal Component Analysis.

Spring'16 **Digital Image Watermarking**.

Mentor: *Prof. Vikram Gadre*, IIT-B.

- Embedded a visually invisible watermark in an image using Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD), and extracted it successfully even after addition of noise.

Work Experience

June'17– June'18 **Software Engineer**, *Samsung R&D Institute*, Banglore.
Developed real time multimedia solutions using digital image processing and machine learning techniques. Part of Camera Solutions team in Multimedia divison of Samsung.

Summer'16 **Software Engineer Intern**, *Samsung R&D Institute*, Banglore.
Mentor: *Karthik Narayanan*
Implemented a system that detects the presence of makeup in face images by extracting features from different regions of face and feeding them to SVM based classifiers.

Summer'15 **Academic team Member**, *International Physics Olympiad (IPhO)*, Mumbai.
Part of the examination panel of IPhO. Evaluated participants' responses to the theory questions. Involved in the arbitration session of theory papers with team leaders of different countries.

2014-17 **Teaching Assistant**, *Indian Institute of Technology Bombay*.

○ Programming and Utilisation, CS101, IIT-B	Autumn'16
○ Quantum Information and Computing, NPTEL (E-learning platform)	Autumn'16
○ Linear Algebra, MA106, IIT-B	Spring'16,'17
○ Calculus, MA105, IIT-B	Autumn'14

Key Courses Taken

- **Cryptography and Security:** Theoretical Foundations of Cryptography, Advanced Cryptography and Network Security, Principles of Data and System Security, Number Theory and Cryptography
- **Learning Algorithms:** Intelligent and Learning Agents, Foundations of Machine Learning, Science of Information and Learning
- **Mathematics:** Linear Algebra, Calculus, Differential Equations, Data Analysis and Interpretation, Probability and Random Processes
- **Other Courses:** Quantum Information and Computing, Quantum Mechanics and Statistics, Data Networks, Advanced Communication Networks

Extra-Curricular Activities

- Mentored freshmen teams during the summer of 2015 in completing technical projects as an Institute Technical Summer Project (ITSP) Mentor.
- Represented our Hostel in Inter-hostel Volleyball Tournament in 2015.
- Volunteered to teach computer basics to primary school students under Computer Literacy Program, an initiative of National Service Scheme (NSS).
- Had been a part of National Cadet Corps (NCC) during school days.