M. Bhargav Sri Venkatesh

CONTACT INFORMATION

Software Engineer
Samsung R&D Institute, Bangalore

Email: bhargav.svm@outlook.com
Mobile: +91 7506134390

AREAS OF INTEREST

- Cryptanalysis, Secure Computation, Applied Cryptography
- Linear Algebra, Probability Theory, Learning Algorithms

EDUCATION

Indian Institute of Technology Bombay **July'13-April'17**
B.Tech. in *Electrical Engineering* with Honors

- Cumulative Performance Index (CPI) of **8.81** (on a scale of 10)
- Minor in Computer Science and Engineering

PUBLICATIONS

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

B Menezes, C Ashokkumar, **MBS Venkatesh**, B Roy, RP Giri *"An error-tolerant approach for efficient AES key retrieval in the presence of cache prefetching - Experiments, Results, Analysis"*[under review]

RESEARCH PROJECTS

AES Key Retrieval in Cache-based Side Channel Attacks **May'15-Jan'17**
Guide: Prof. Bernard Menezes, IIT Bombay

- The software implementation of AES is an attractive target to cache-based side channel attacks, since it makes extensive use of cache-resident table lookups. We employed a multi-threaded spy process and ensured that each time slice provided to the victim (running AES) is small enough so that it makes a very limited number of table accesses. I have worked on designing a suite of algorithms to deduce the 128-bit AES key using the set of (unordered) cache line numbers captured by the spy threads in an access-driven cache-based side channel attack. I have also developed probability models which explain the results obtained from implementing our algorithms in experiments.

Lattice based Cryptanalysis **Jan'17-May'17**
Guide: Prof. Bernard Menezes, IIT Bombay

- After working on cache-based side channel attacks on AES, I have started working on similar attacks on DSA and ECDSA where required strategies are completely different from earlier one. Here, we deduce partial information of ephemeral keys such as few bits anywhere in the key using sequence of doubles and adds from spy program. Using those known bits, we have formulated a known lattice problem which is hard to solve. I have studied about hard lattice problems, their solvers and tried to employ them in retrieving the secret key. I have worked towards developing algorithms based on lattices, to deduce the secret key with high success rate.

RELEVANT COURSES

- **Cryptography and Security**
  Advanced Network Security and Cryptography — Number Theory and Cryptography
  Theoretical Foundations of Cryptography — Principles of Data and System Security
- **Mathematics and Statistics**
  Machine Learning and Intelligent Agents — Linear Algebra, Matrix Computations
  Probability and Random Processes — Markov Chains and Queuing Systems

Academic Projects

Security Analysis of Remote Voting Systems **July'16-Apr'17**

Guide: Prof. R.K.Shyamasundar, IIT Bombay

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

Intelligent and Learning Agents - Multiple Projects **Autumn 2016**

Guide: Prof : Shivaram Kalyanakrishnan

Course: Foundations of Learning Agents

- Developed an agent to play the game of carrom, in single player mode as well as in a two-player mode. Used neural networks to predict Q-values due to continuous state and action space. Trained another agent using heuristic strategies [report].
- Explored various strategies in developing an agent to optimise number of heads, where you are given N coins which may be biased.
- Created an optimal agent for a given MDP, using policy improvement and policy evaluation which are standard methods in reinforcement learning.

Internship

Face Makeup Detection System **May'16-July'16**

Mentor: Karthik Narayanan, Samsung R&D Institute, Bangalore

- During my internship, I have worked on an interesting machine learning problem. My task is to identify the kind of makeup applied to the face of a woman. I have extracted different features like Color moments, GIST, Edge oriented histogram and LBP (Linear Binary Patterns) from the images. And then trained SVM (Support Vector Machine) based classifiers using those features. Classification accuracy of 80% is achieved. Used OpenCV to implement the method.

Other Projects

- Object classification using neural networks.
- Developed a chrome extension which hides key strokes of user and performs password hashing based on domain name, which can thwart attacks based on social engineering.
- Reading project on Oblivious transfer and Yao's garbled circuits protocols.

Achievements

- **AA grade** for distinctive performance in **Computer and Network Security**, **Quantum Computing and Information** and many other courses. *(2015)*
- **A**dvanced **P**erformance grade in **Linear Algebra** course. *(2014)*
- **All India Rank 7** in **JEE Mains**-II. *(2013)*
- Received prestigious **KVPY Scholarship**, Indian Institute of Science. *(2012)*
- **All India Rank 9** in National level Mathematics Test by **AMTI**, India. *(2012)*
- **Gold Medal** from Department of Science and Technology, Govt. of India and received **INTEL Award of Excellence** for overall best performance and for securing **First Rank** in **IGNOU-UNESCO Science Olympiad**. *(2011)*

Professional Experience

Samsung R&D Institute, Bangalore **June'17-Present**

- Software Engineer in Multimedia team of Samsung, Bangalore

Teaching Experience

Indian Institute of Technology Bombay

- Programming and Utilisation, CS101 **Autumn 2016**
- Quantum Information and Computing, NPTEL **Autumn 2016**
- Linear Algebra, MA106 **Spring 2016, 2017**
- Calculus, MA105 **Autumn 2014**