Vivek Arte | Curriculum Vitae

contact@vivekarte.in • vivekarte.in

Research Interests

Cryptography, Zero-Knowledge, Private Set Intersection, Applied Cryptography, Computer Security

Education

University of California San Diego, La Jolla, CA, USA
Master of Science in Computer Science *2018 - 2021*
Academic Advisor: Prof. Mihir Bellare.

- **GPA** = 4.0/4.0
- **Research Topic**: What are we PSIgning up for? Analyzing Applications of Two-Party Private Set Intersection

Takshashila Institution, Bengaluru, India
Graduate Certificate in Public Policy (Technology and Policy) *2021*

- **Overall Grade** : A

Indian Institute of Technology (IIT) - Bombay, Mumbai, India
Bachelor of Technology in Electrical Engineering, Master of Technology in Electrical Engineering *2013-2018*
Dual-Degree Program - Specialization in Microelectronics

- **Minor** in Department of **Computer Science and Engineering** – **CGPA** = 9.60/10
- **Major CGPA** = 9.39/10

Publications

Dual-Mode NIZKs : Possibility and Impossibility Results for Property Transfer INDOCRYPT 2020
Incremental Cryptography Revisited: PRFs, Nonces and Modular Design INDOCRYPT 2020

Research Projects

Concrete Security for Zero-Knowledge
UC San Diego *October 2018 - December 2020*
Guide: *Prof. Mihir Bellare.*

- Surveyed the area of Zero-Knowledge Proofs and Arguments to compare the performance and benefits of different schemes
- Studied the transference of properties between modes in dual-mode NIZK proof systems, and their implications for applications. [ePrint Full Version]
- Provided a concrete security proof of the Naor-Yung scheme for IND-CCA secure public-key encryption using a non-interactive zero knowledge proof system

Concrete Security for Private Set Intersection
Galois, Inc. *June 2020 - September 2020*
Guides: *Alex Malozemoff, Dave Archer.*

- Surveyed the area of Private Set Intersection (PSI) protocols to understand the different techniques and primitives used in their construction
- Defined indistinguishability-based notions for semi-honest and malicious PSI in order to improve protocol efficiency at minimal cost to security
- Studied the construction of a fully malicious-secure PSI protocol from 1-out-of-2 oblivious transfer

Incremental Pseudorandom Functions
UC San Diego *January 2019 - September 2020*
Guide: *Prof. Mihir Bellare.*

- Defined security notions for incremental PRFs and incremental message authentication schemes.
- Analyzed the relations between different security notions, and provided generic transforms to obtain security in a multi-document setting from a scheme secure in the single-document setting.
- Extended the Carter-Wegman paradigm of almost-universality to the incremental setting. [ePrint Full Version]

Voltage Controlled Entanglement Switch
IIT Bombay *January 2017 - June 2018*
Guides: *Prof. Bhaskaran Muralidharan, Prof. Sai Vinjanampathy.*

- Designed a device that generates entanglement between two qubits when a voltage is passed through a quantum dot system.
- Applied Quantum Transport and Quantum Information concepts to study the characteristics of the device under different conditions.

Spin-Torque and Applications to Quantum Computing
IIT Bombay *July 2016 - December 2016*
Guide: *Prof. Bhaskaran Muralidharan.*

- Studied Quantum Transport and Current Flow through Nanotransistors.
- Studied the application of spin-torque effects to quantum processes involving single qubit rotation as well as two qubit entanglement.
- Modelled the use of large number of electrons with specific spin potential to produce the desired qubit operations.

Modelling Changes in Flight Scheduling on the Introduction of Scheduling Constraints
Thayer School of Engineering at Dartmouth *Summer 2016*
Guide: *Prof. Vikrant Vaze.*

- Analyzed the data of flight schedules from 2005 to 2015 at the three New York City area airports (Newark Liberty International Airport, LaGuardia Airport, and John F. Kennedy International Airport).
- Developed a predictive model, using Support Vector Machines to train on the available data, and predict changes in flight scheduling when similar rule changes take place.
- Developed code to analyze and classify data from the Aviation Systems Performance Metrics (ASPM) system and generalized it for simple extension to further data.

Proving the Security of a Modified TLS Implementation
Tel Aviv University *Summer 2015*
Guide: *Prof. Ran Canetti.*

- Studied the implementation of the Transport Layer Security (TLS) Protocol, along with attacks, especially the Downgrade Attack.
- Suggested a modification to TLS which would be resistant to the Downgrade Attack.
- Studied the Universal Composability (UC) Model of Security and worked on using the UC Model to prove the security of this modified version of TLS.

Key Academic Achievements

- *Received the* **Institute Academic Prize** *from* IIT Bombay *in* 2015.
- **All India Rank 36** *out of 1.3 million students in* IIT-JEE (Main) 2013. **All India Rank 213** *out of 150,000 students in* IIT-JEE (Advanced) 2013.
- *Cleared the* Indian National **Astronomy** Olympiad – Junior Level in 2010, Senior Level in 2013. *Was among the top students selected for the* **International Olympiad Training Camp**.
- *Ranked* **6th** *among participants from* 8 South Asian Nations *at the* **IGNOU-UNESCO Science Olympiad**, 2011. Also was the **Chemistry Subject Topper**.
- **11th** *rank in* India *in the* **Kishore Vaigyanik Protsahan Yojana (KVPY) Fellowship**, 2011, *funded by the* Department of Science and Technology, Government of India.
- **5th** *rank in* India *in the* **National Talent Search Examination (NTSE)**, 2009, *organized by* NCERT, Government of India.
- *Received the* **Dr. Homi Bhabha Young Scientist Award**, Gold Medal *in* 2006, and Silver Medal *in* 2009, from among 40,000 students in the Greater Mumbai Region.

Course Projects

Using Fully Homomorphic Encryption libraries
Course: Advanced Cryptography, UC San Diego *Fall 2020*

- Studied and implemented basic progams in $\Lambda \circ \lambda$, an open source library in Template Haskell that implements fully homomorphic encryption schemes and other lattice cryptography primitives.
- Looking at reimplementing $\Lambda \circ \lambda$ using a language with support for dependent and refinement types.

Program Analysis using LLVM
Course: Advanced Compiler Design, UC San Diego *Winter 2020*

- Implemented a generic intra-procedural dataflow analysis framework and used it to implement reaching definition analyses, liveness analyses, and pointer analyses.
- Implemented an inter-procedural modified global variables analysis and constant propagation analysis.

Reflections on Trusting Rust : A RustBelt Experience Report
Course: Computer Security, UC San Diego *Spring 2019*

- Studied the RustBelt project, which developed λ-Rust to provide a formal proof of correctness of the Rust type system via the Iris framework in Coq.
- Extended RustBelt with an implementation of the Rust vector type, and provided a sample verification of a function from the vector library.

Indistinguishability Obfuscation from Trilinear Maps and Block-Wise Local PRGs
Course: Advanced Tools from Modern Cryptography, IIT Bombay *Fall 2017*

- Reviewed the paper published in CRYPTO 2017 by Huijia Lin and Stefano Tessaro.
- Studied a technique to obtain compact functional encryption (FE) from FE for degree-L polynomials.
- Understood a bootstrapping technique to achieve indistinguishability obfuscation for polynomial-sized circuits from this compact FE scheme

Analysis of the Dragon Stream Cipher
Course: An Introduction to Number Theory and Cryptography, IIT Bombay *Spring 2017*

Accelerating Rational Arithmetic on an FPGA
Course: VLSI Design Lab, IIT Bombay *Spring 2017*

Technical Skills

C++, Python, Haskell, Rust, LLVM, MATLAB, Verilog HDL, VHDL, LaTeX

Teaching

- **Teaching Assistant - Introduction to Modern Cryptography** - UC San Diego, *FA19, SP20*
  - Helped design assignment questions and generate autograder scripts for programming assignments.
  - Conducted discussion sections to help students understand lecture concepts through problem solving.
  - Conducted office hours to clarify student doubts. Also responsible for grading examinations for the course.
- **Teaching Assistant - Design and Analysis of Algorithms** - UC San Diego, *WI20*
  - Designed autograder scripts for programming assignments.
  - Conducted office hours to clarify student doubts. Also responsible for grading examinations for the course.
- **Teaching Assistant - Introduction to Number Theory and Cryptography** - IIT Bombay, *Spring 2018*
  - Selected as an Undergraduate TA for a course catering to about 90 students.
  - Conducted office hours to clarify student doubts. Also responsible for grading examinations for the course.
  - Received a **Certificate of Appreciation for Excellence in Teaching Assistantship** from the Department of Electrical Engineering, IIT Bombay.
- **Teaching Assistant - Microprocessors Lab** - IIT Bombay, *Autumn 2017*
  - Selected as an Undergraduate TA for a course catering to about 140 students.
  - Helped clarify doubts and concepts for the students. Also responsible for grading assignments.
  - Guided students in implementing a Tone Generator using an 8051 microcontroller and an ADC.
  - Guided students through the design of a RISC microprocessor, implementation of the design using VHDL, and testing on an FPGA.
  - Received a **Certificate of Appreciation for Excellence in Teaching Assistantship** from the Department of Electrical Engineering, IIT Bombay.

Standardized Test Scores

- **GRE**: 340/340 (Quantitative: 170, Verbal: 170, Analytical Writing: 5.0/6.0)
- **TOEFL**: 117/120 (Reading: 30, Listening: 30, Speaking: 27, Writing: 30)