|  |  |
| --- | --- |
| Nikhil Pappu | horizontal line Nikhil Pappu Email: [nkhlpappu@gmail.com](mailto:nkhlpappu@gmail.com)  Website: <http://nikhilpappu.info/>  5th year Integrated M. Tech (5yr Bachelors + Masters) student in Computer Science and Engineering at the International Institute of Information Technology, Bangalore (IIIT-B), India. |
| **ㅡ** Interests | horizontal line   * Secure Multiparty Computation * Cryptography * Distributed Computing * Blockchain |
| **ㅡ** **Experience** | horizontal line Research in Multiparty Computation / Capstone Project2020-21, International Institute of Information Technology, BangaloreAdvisor: [Ashish Choudhury](https://sites.google.com/site/ashishcrypto/) Studied information-theoretic multiparty computation tolerating a generalized non-threshold adversary in the asynchronous communication setting. Submitted some of our results in a paper titled *Perfectly-Secure Asynchronous MPC for General Adversaries*, which has been accepted to *Indocrypt 2020*. Prior to this work, had worked on constructing an efficient 4 party privacy preserving ML protocol tolerating a general adversary, where the protocol is resilient to a stronger adversary compared to honest majority protocols but avoids relatively slow public key operations required by dishonest majority protocols. Teaching Assistant / CC112: Discrete Mathematics2020-21, International Institute of Information Technology, BangaloreInstructor: [Ashish Choudhury](https://sites.google.com/site/ashishcrypto/) Prepared and evaluated graded assignments for various subtopics and conducted tutorial sessions for discussing their solutions for a class of 100 sophomores. Open Source Developer - Google Summer of Code 2018Summer 2018, [SymPy](https://www.sympy.org/): a Python library for symbolic mathematics. Implemented a parser that translates Autolev (a proprietary symbolic dynamics language, now superseded by [MotionGenesis](http://www.motiongenesis.com/)) code to SymPy code using the ANTLR parser generator. The project involved creating an appropriate grammar to parse Autolev code, writing Python and SymPy code that is executed during parse tree traversals, writing tests and documentation among other things. More details [here](https://summerofcode.withgoogle.com/archive/2018/projects/6339390586486784/) and [here](https://github.com/sympy/sympy/wiki/GSoC-2018-Report). |
| **ㅡ** **Education** | horizontal line International Institute of Information Technology, Bangalore (IIIT-B) / Integrated M. Tech in Computer Science and Engineering2016- CGPA: 3.34/4 (8/10 semesters)  Specialization in Theoretical Computer Science FIITJEE Junior College / Grade XI & XII2014-2016, Narayanguda, Hyderabad Studied Math, Physics and Chemistry; 97.7%; JEE Main Rank: 5995 |
| **ㅡ** Writings | horizontal line  **Perfectly-Secure Asynchronous MPC for General Adversaries**  Ashish Choudhury, Nikhil Pappu  *Accepted to Indocrypt 2020* |

|  |  |
| --- | --- |
| **ㅡ** Programming **Skills** | horizontal line  **General:** Python, C, C++, Java, OCaml  **Web Dev:** HTML5, CSS, Javascript, Node.js, React  **ML:** R, scikit-learn, GNU Octave  **DBMS:** MySQL, SQLite, MongoDB  **DevOps:** Git, Jenkins, Docker, ELK stack  **Misc:** Android, LaTeX, R Markdown, bash/shell, cryptoTools, OpenGL, SymPy |