

# ARKA RAI CHOUDHURI

**Email:** achoud@cs.jhu.edu

## RESEARCH INTEREST

My primary research interest is in **theoretical cryptography**. I am also interested in some other aspects of theoretical computer science.

## EDUCATION

**Ph.D.** in Computer Science 2016-present  
Johns Hopkins University  
CGPA: 4.0/4.0  
Advisor: Abhishek Jain

**Master of Technology** in Computer Science 2014-2016  
Indian Statistical Institute, Kolkata  
Aggregate Marks: 93.3 %  
Rank 1/28  
Thesis: Salsa and ChaCha: An Improved Analysis  
*Sunity Kumar Pal Gold Medal* for best dissertation  
*ISIAA-Rashi Ray Memorial Gold Medal* for outstanding performance

**Bachelor of Technology** in Computer Science 2010-2014  
National Institute of Technology Karnataka, Surathkal  
CGPA: 8.53

## PUBLICATIONS

- Prabhanjan Ananth, Arka Rai Choudhuri, Abhishek Jain, “*A New Approach to Round-Optimal Secure Multiparty Computation*”. CRYPTO 2017.
- Arka Rai Choudhuri, Subhamoy Maitra, “Significantly Improved Multi-bit Differentials for Reduced Round Salsa and ChaCha”. FSE 2017/ ToSC 2016.

## PROFESSIONAL ACTIVITIES

External reviewer for: EUROCRYPT’16, PKC’17, CRYPTO’17

## SCHOLASTIC ACHIEVEMENTS

- *Sunity Kumar Pal Gold Medal* for best dissertation in M.Tech (CS) programme 2014-16.
- *ISIAA-Rashi Ray Memorial Gold Medal* for outstanding performance in M.Tech (CS) programme 2014-16.
- Rank 1 (out of 28) in M.Tech Computer Science at Indian Statistical Institute Kolkata.
- Selected for the Summer@EPFL research internship programme for the summer of 2015.
- Placed 10<sup>th</sup> in the country in the National Cyber Olympiad for the year 2010.
- Selected as Summer Research Fellow by the Indian Academy of Sciences for the summer of 2013.
- Reached the national round of the National Talent Search Examination of 2008. Awarded the state scholarship for the same.

## **SCHOOLS AND CONFERENCES**

- Winter School on *Interplay Between Statistics and Cryptology* December 2014, at Indian Statistical Institute.
- Workshop on *Number Theory and Cryptology* held at National Institute of Technology Karnataka, Surathkal in 2013.
- *IC Research Day 2015* held at EPFL during the summer of 2015.
- *Yahoo! Summer School for Information Retrieval and the Semantic Web* held at Indian Institute of Science during the summer of 2013.
- Participant at the *Turing Centenary Conference* held at PESIT Bangalore during the summer of 2012.

## **Languages**

Fluent in English and Bengali. Have a good working knowledge of Hindi and Kannada.

## **EXTRACURRICULAR ACTIVITIES**

- Was captain of the University football (soccer) team at National Institute of Technology for the academic year 2013-14.
- Trained in Hindustani classical Tabla for 7 years.
- Member of the Literary, Stage and Debating society at NITK as a part of the quiz team.
- Head of the computer special interest group of the Institution of Engineers, NITK chapter for the year 2013-14.