Sanjay Bhattacherjee

Visiting Scientist,
Turing Lab,
Applied Statistics Unit,
Indian Statistical Institute,
Kolkata, India.
sanjay.bhattacherjee@gmail.com

I defended my PhD thesis titled "Tree-Based Symmetric Key Broadcast Encryption" on 8^{th} October, 2015. My PhD supervisor was Prof. Palash Sarkar.

1 Research

Public Key Trace and Revoke

1. with Shweta Agrawal and Duong Hieu Phan and Damien Stehlé and Shota Yamada. Efficient Public Trace and Revoke from Standard Assumptions, *in submission.*

Symmetric Key Broadcast Encryption

2. [**Journal**] with Palash Sarkar. Reducing Communication Overhead of the Subset Difference Broadcast Encryption Scheme. **IEEE Transactions on Computers**, **IEEE Transactions on Computers**, 65(8): 2575-2587 (2016).
(A very brief summary of this work was presented at the ECC 2014 rump session.)

3. [**Journal**] with Palash Sarkar. Tree Based Symmetric Key Broadcast Encryption. **Journal of Discrete Algorithms**, 34:78-107, 2015.
(A very brief summary of this work was presented at the Asiacrypt 2013 rump session.)

4. [**Journal**] with Palash Sarkar. Concrete Analysis and Trade-Offs for the (Complete Tree) Layered Subset Difference Broadcast Encryption Scheme. **IEEE Transactions on Computers**, 63(7):1709-1722, 2014.

5. [**Journal**] with Palash Sarkar. Complete Tree Subset Difference Broadcast Encryption Scheme and its Analysis. **Design, Codes and Cryptography**, Volume 66, Issue 1 (2013), Page 335-362.

6. [**Workshop**] with Palash Sarkar. An Analysis of the Naor-Naor-Lotspiech Subset Difference Algorithm. **Proceedings of the 7th International Workshop on Coding and Cryptography**, Paris, April 11-15, 2011.

VLSI Design Verification

7. [**Conference**] with Santanu Bhowmick and Nandakumar G.N. Generation of Test Vectors for Sequential Cell Verification. **ARM Regional Engineering Conference**, 2008.

2 Academic Degrees

- **Doctor of Philosophy in Computer Science** from Indian Statistical Institute, 2015.
- **Master of Technology in Computer Science** from Indian Statistical Institute, 2009.
- **Bachelor of Engineering in Information Technology** from Jadavpur University, 2005.

3 Work Experience

Academia

1. **Indian Statistical Institute, Kolkata** (www.isical.ac.in)
   Visiting Scientist; since December, 2016.
   Projects:
   - (In preparation) On Bitcoins and Blockchains.
   - (In preperation) On voting games.
   - (In preperation) On side-channel analysis.
2. **École Normale Supérieure de Lyon** (www.ens-lyon.fr)
   Post-doc; February, 2015 - November, 2016.
   Projects:
   - (Completed) A significant revision of the final work of my PhD thesis for reducing the communication overhead of the NNL-SD scheme. We added parameters for trade-off between the NNL-SD scheme and the case where every subset is assigned a key. The average header length achieved by the new schemes for each parameter choice is smaller than all known schemes having the same decryption time as that of the NNL-SD scheme and achieving non-trivial trade-offs between the user storage and the header size. However, the amount of key material that a user is required to store increases.
   - (In submission) On designing algebraic trace-and-revoke schemes that allow public traceability, using functional encryption primitives. We are able to obtain *public traceability and revocation at the same time* in the bounded collusion model using standard assumptions. This is a very desirable combination for practical usage of the schemes. To the best of our knowledge, such combination of properties was not known before and our schemes are more efficient than all existing algebraic schemes. This work has already been presented here.

Industry

1. **Dynamic Digital Technology Private Limited, Kolkata** (www.polarisnetworks.net)
   Networking Developer; July, 2006 - July, 2007.
   Client: Rippletech Technologies, Inc. (was acquired by NitroSecurity in 2008; NitroSecurity was

further acquired by McAfee (Intel Security) in 2011)
Product: Informant (now part of the McAfee Database Activity Monitoring tool)
Responsibilities: (In a team of 6)

- Networking Developer: I developed new modules for packet parsing, memory management, etc. For a considerable amount of time I was the sole developer in the team.
- Maintaining the existing packet parsing modules.

Achievements: I proposed and executed two major design changes in the product:

- Completely redesigned the protocol parser module for the proprietary TNS protocol underlying Oracle DBMS to make it more generic and robust towards packet parsing. Since the TNS protocol specifications are not public, it had to be reverse-engineered based on our knowledge of the other database protocols.
- Redesigned the memory leak module that resulted in better efficiency in detecting and hence logging memory leaks at run time.

2. **Infosys Technologies Limited, Bengaluru** (www.infosys.com)
Software Engineer; June, 2005 - June, 2006.
Client: Nortel
Product: GSM Switch Software
Responsibilities: (In a team of 52) Writing C++ programs that were fed to an Automation Platform that would simulate the messaging and other functions of DMS Mobile Switching Center Switches for GSM Mobiles.

4 Internships

1. **Indian Institute of Science, Bengaluru** (http://www.iisc.ernet.in)
March, 2013 - April, 2013.
A short academic visit exploring "forward security" in broadcast encryption with Dr. Sanjit Chatterjee.

2. **ARM Embedded Technologies Private Limited, Bengaluru** (www.arm.com)
May, 2008 - July, 2008.
We (Santanu Bhowmick, Nandakumar G N and myself) devised an algorithm for generation of a minimal set of test vectors for Sequential Cells. This work led to a paper that has been published in ARM Regional Engineering Conference (internal to ARM).

3. **Indian Statistical Institute, Kolkata** (www.isical.ac.in)
June, 2004 - August, 2004.
I worked under the supervision of Dr. Bibhas Chandra Dhara and Prof. Bhabatosh Chanda in designing and implementing some improvements to Image and Video Compression and Decompression algorithms.

5 Teaching

1. **Cryptologie à clé publique** at ISFA, Université de Lyon 1 (UCBL)
   Master Pro course; February 2016.
   Jointly with Prof. Fabien Laguillaumie.

2. **Topics in Algebra** (Tutorial Classes) at ISI, Kolkata.
   M.Tech.(CS); 2011.
   Course taken by Prof. Palash Sarkar.

3. **Programming Languages and Methodology** at ISI, Kolkata.
   M.Tech.(CS); 2009, 2010.
   Jointly with Prof. Subhamoy Maitra.

4. **Topics in Algorithms** at Ramakrishna Mission Vidyamandira, Belur.
   B.Sc.(CS); 2009, 2010.

5. **Data Structures** at Ramakrishna Mission Vidyamandira, Belur.
   B.Sc.(CS); 2009, 2010.