Aniket Kate

Cluster of Excellence, Saarland University
Saarbruecken, Germany
http://people.mmci.uni-saarland.de/~aniket
aniket@mmci.uni-saarland.de
Twitter: @aniketpkate

Campus E1.7, Room 216
Saarland University
66123 Saarbruecken
Germany
Office: +49-681-302-71939

EDUCATION

University of Waterloo — Waterloo, Canada
Ph.D. in Computer Science — Sep 2006–Jun 2010
Thesis title: *Distributed Key Generation and its Applications*
Supervisor: *Ian Goldberg*

Indian Institute of Technology (IIT)—Bombay — Mumbai, India
M.Tech. in Computer Science and Engineering — Aug 2004–Jun 2006

Mumbai University — Mumbai, India
B.E. in Information Technology — Aug 1999–Jul 2003

RESEARCH INTEREST

I am an applied cryptographer and a privacy researcher. My current research projects focuses on developing (provably secure) cryptographic systems for privacy and distributed trust.

RESEARCH EXPERIENCE

Cluster of Excellence, Saarland University — Saarbruecken, Germany
Leader, Cryptographic Systems Research Group — Aug 2012–*Present*

Max Planck Institute for Software Systems (MPI-SWS) — Saarbruecken, Germany
Postdoctoral Researcher with Michael Backes — Sep 2010–July 2012

University of Waterloo — Waterloo, Canada
Research Assistant with Ian Goldberg — May 2007–Aug 2010
Research Assistant with Urs Hengartner — Sep 2006–Apr 2007

SELECTED PROJECTS

- **Privacy in Cryptocurrencies and Payment Networks**
  Designed and implemented protocols for providing unlinkability among senders and receivers of Bitcoin transactions as well as of payments over payment networks
  Work published at ESORICS'14 and NDSS'15
- **Analyzing and Improving Anonymous Communication Networks**
  Formalized important anonymity properties as well as anonymous communication networks (ACNs) such as Tor, and analyzed (and quantified) anonymity provided by Tor in practice
  Work published at CSF'12, CSF'13, and CCS'14
- **Cryptography for Anonymity**
  Designed and implemented several one-way anonymous one-way authenticated key exchange (1W-AKE) schemes for ACNs to acheive computational efficiency, scalability, UC-security as well as accountability
  Work published at PETS'07, FC'10, WPES'12, ACNS'14, NIST PQC'15, and in TISSec.
- **Using Trusted Hardware for Privacy-preserving and Distributed Systems**
  Demonstrated the utility of trusted hardware towards solving the problem of privacy-preserving online advertising, and towards improving the resiliency of distributed protocol in the form of non-equivocation
  Work published as Oakland'12, PODC'12, PODC'14, and NDSS'15

◇ **Computational Verifiable Secret Sharing**
Improved communication efficiency and resilience of computational verifiable secret sharing, and simplified the cryptographic trust assumption required for the same
Work published at Asiacrypt'10, Asiacrypt'11, CT-RSA'13, and PODC'14.

◇ **Distributed Key Generation and its Applications**
Designed and implemented a distributed key generation (DKG) protocol for establishing distributed (cryptographic) trust over the Internet, and explored its applications to distributed hash tables (DHTs), identity-based cryptography, and password authentication protocols
Work published at ICDCS'09 and ICDCS'10, SCN'10, ASIACCS'12, and in ACM/IEEE ToN.

REFEREED PUBLICATIONS

Papers with alphabetical author ordering are marked with ⟨ABC✎⟩. All other papers follow the contribution-based author ordering.

1 "Data Lineage in Malicious Environments"
Michael Backes, Niklas Grimm, and Aniket Kate ⟨ABC✎⟩
To appear in *IEEE Transactions on Dependable and Secure Computing (***TDSC)**, 2015

2 "Visigoth Fault Tolerance"
Daniel Porto, Joao Leitao, Cheng Li, Allen Clement, Aniket Kate, Flavio Junqueira, and Rodrigo Rodrigues
To appear at *European Conference on Computer Systems (***EuroSys)**, April 2015

3 "Privacy Preserving Payments in Credit Networks"
Pedro Moreno-Sanchez, Aniket Kate, Matteo Maffei, and Kim Pecina
To appear at *Network and Distributed System Security Symposium (***NDSS)**, Feb 2015

4 "Privacy-preserving Data Aggregation with Optimal Utility"
Fabienne Eigner, Aniket Kate, Matteo Maffei, Francesca Pampaloni, and Ivan Pryvalov ⟨ABC✎⟩
30th *Annual Computer Security Applications Conference (***ACSAC)**, Dec 2014

5 "(Nothing else) MATor(s): Monitoring the Anonymity of Tor's Path Selection"
Michael Backes, Aniket Kate, Sebastian Meiser, and Esfandiar Mohammadi ⟨ABC✎⟩
21st *ACM Conference on Computer and Communications Security (***CCS)**, Nov 2014

6 "CoinShuffle: Practical Decrentralized Coin Mixing for Bitcoin"
Tim Ruffing, Pedro Moreno-Sanchez, and Aniket Kate
19th *European Symposium on Research in Computer Security (***ESORICS)**, Sep 2014

7 "Lime: Data Lineage in the Malicious Environment"
Michael Backes, Niklas Grimm, and Aniket Kate ⟨ABC✎⟩
10th *International Workshop on Security and Trust Management (***STM)**, Sep 2014

8 "Asynchronous MPC with a Strict Honest Majority Using Non-equivocation"
Michael Backes, Fabian Bendun, Ashish Choudhury, and Aniket Kate ⟨ABC✎⟩
33rd *ACM Symposium on Principles of Distributed Computing (***PODC)**, July 2014

9 "Introducing Accountability to Anonymity Networks"
Michael Backes, Jeremy Clark, Peter Druschel, Aniket Kate, and Milivoj Simeonovski ⟨ABC✎⟩
12th *International Conference on Applied Cryptography and Network Security (***ACNS)**, June 2014

10 "AnoA: A Framework For Analyzing Anonymous Communication Protocols"
Michael Backes, Aniket Kate, Praveen Manoharan, Esfandiar Mohammadi, and Sebastian Meiser ⟨ABC✎⟩
26th *IEEE Computer Security Foundations Symposium (***CSF)**, June 2013

11 "Towards Practical Communication in Byzantine-Resistant DHTs"
Maxwell Young, Aniket Kate, Ian Goldberg, and Martin Karsten
*IEEE/ACM Transactions on Networking (***ToN)**, 21(1), Feb 2013

12 "Asynchronous Computational VSS with Reduced Communication Complexity"
Michael Backes, Amit Datta, and Aniket Kate ⟨ABC✎⟩
*Cryptographers' Track - RSA Conference (***CT-RSA)**, Feb 2013

13 "An Efficient Key-Exchange Protocol for Onion Routing"
Michael Backes, Aniket Kate, and Esfandiar Mohammadi ⟨ABC✎⟩
11th *ACM Workshop on Privacy in the Electronic Society (***WPES)**, Oct 2012

14 "On the (Limited) Power of Non-Equivocation"
Allen Clement, Flavio Junqueira, Aniket Kate, and Rodrigo Rodrigues ⟨ABC✎⟩
31*st ACM Symposium on Principles of Distributed Computing (***PODC)**, Jul 2012

15 "Provably Secure and Practical Onion Routing"
Michael Backes, Ian Goldberg, Aniket Kate, and Esfandiar Mohammadi ⟨ABC✎⟩
25*th IEEE Computer Security Foundations Symposium (***CSF)**, Jun 2012

16 "ObliviAd: Provably Secure and Practical Online Behavioral Advertising"
Michael Backes, Aniket Kate, Matteo Maffei, and Kim Pecina ⟨ABC✎⟩
33*rd IEEE Symposium on Security and Privacy (***Oakland)**, May 2012

17 "Adding Query Privacy to Robust DHTs"
Michael Backes, Ian Goldberg, Aniket Kate, and Tomas Toft ⟨ABC✎⟩
7*th ACM Symposium on Information, Computer and Communications Security (***ASIACCS)**, May 2012.

18 "Computational Verifiable Secret Sharing Revisited"
Michael Backes, Aniket Kate, and Arpita Patra ⟨ABC✎⟩
17*th International Conference on the Theory and Application of Cryptology (***ASIACRYPT)**, Dec 2011.

19 "Generalizing Cryptosystems Based on the Subset Sum Problem"
Aniket Kate and Ian Goldberg
*Springer International Journal of Information Security (***IJIS)***, 10 (3)*, May 2011.

20 "Pairing-Based Onion Routing with Improved Forward Secrecy"
Aniket Kate, Gregory M. Zaverucha, and Ian Goldberg
*ACM Transactions on Information and System Security (***TISSEC)***, 13(4)*, Dec 2010

21 "Constant-Size Commitments to Polynomials and Their Applications"
Aniket Kate, Gregory M. Zaverucha, and Ian Goldberg
16*th International Conference on the Theory and Application of Cryptology (***ASIACRYPT)**, Dec 2010

22 "Distributed Private-Key Generators for Identity-Based Cryptography"
Aniket Kate and Ian Goldberg
7*th Conference on Security and Cryptography for Networks (***SCN)**, Sep 2010

23 "Practical Robust Communication in DHTs Tolerating a Byzantine Adversary"
Maxwell Young, Aniket Kate, Ian Goldberg, and Martin Karsten
30*th International Conference on Distributed Computing Systems (***ICDCS)**, Jun 2010

24 "Using Sphinx to Improve Onion Routing Circuit Construction"
Aniket Kate and Ian Goldberg
14*th International Conference on Financial Cryptography and Data Security (***FC)**, Jan 2010

25 "Distributed Key Generation for the Internet"
Aniket Kate and Ian Goldberg
In 29*th International Conference on Distributed Computing Systems (***ICDCS)**, Jun 2009

26 "Anonymity and Security in Delay Tolerant Networks"
Aniket Kate, Gregory M. Zaverucha, and Urs Hengartner
3*rd International Conf. on Security and Privacy in Communication Networks (***SecureComm)**, Sep 2007.

27 "Pairing-Based Onion Routing"
Aniket Kate, Gregory M. Zaverucha, and Ian Goldberg
7*th Privacy Enhancing Technologies Symposium (***PET)**, Jun 2007.

OTHER REFERRED PUBLICATIONS

28 "Post-Quantum Forward Secure Onion Routing (Future Anonymity in Today's Budget)"
Satrajit Ghosh and Aniket Kate
To appear at *NIST Workshop on Cybersecurity in a Post-Quantum World (***NIST PQC)**, April 2015.

29 "Identity-Based Steganography and Its Applications to Censorship Resistance"
Tim Ruffing, Jonas Schneider, Aniket Kate
6*th Workshop on Hot Topics in Privacy Enhancing Technologies (***HotPETs)**, Jul 2013.

30 "Brief Announcement: Distributed Cryptography using TrInc"
Michael Backes, Fabian Bendun, and Aniket Kate ⟨ABC⟩
31*st ACM Symposium on Principles of Distributed Computing (***PODC)**, Jul 2012.

31 Aniket Pundlik Kate: "Distributed Key Generation and Its Applications"
PhD Thesis, University of Waterloo, Jun 2010.

32 Aniket Kate: "Frobenius Endomorphism Based Cryptosystems"
Master Thesis, Indian Institute of Technology (IIT)—Bombay, Jun 2006.

SELECTED INVITED TALKS

- "Anonymous Communication Networks: Design, Analysis and Challenges" at TU Dresden, Germany. Sep 2014.
- "Differential Guarantees for Cryptographic Systems" at Microsoft Research, India. Apr 2014.
- "Asynchronous MPC with a Strict Honest Majority Using Non-equivocation" at Applied Multi-Party Computation Workshop, Microsoft Research, Redmond, USA. Feb 2014.
- "Introducing Accountability to Onion Routing" at *Grande Region Security and Reliability Day (GRSRD 2013)*. Apr 2013.
- "Towards Practical and Efficient Distributed Trust" at *Indian Institute of Technology-Kharagpur (IIT-Kgp)*, India. Sep 2012.
- "An Interplay between Anonymity, Privacy, and Accountability" at *Indian Statistical Institute (ISI), Kolkata*, India. Sep 2012.
- "Recent Improvements to Onion Routing" at *IBM Research - Zurich*, Rueschlikon, Switzerland. Jan 2012.
- "Recent Improvements in Onion Routing Circuit Construction" in the *Laboratory of Algorithmics, Cryptology and Security (LACS), University of Luxembourg*, Luxembourg. Feb 2010.
- "Anonymous Key Agreement in an Identity-based Infrastructure and Applications" at the *MITACS 2009 Annual Conference*, Canada. Jun 2009.

SUPERVISION EXPERIENCE

PhD Students

Tim Ruffing	Summer 2013–*Present*
Pedro Moreno-Sanchez	Winter 2013/14–*Present*

Master Thesis Student

Tobias Theobald	Winter 2014/15–*Present*
Simon Heinzel	Winter 2014/15–*Present*
Uzair Mahmood	Winter 2014/15–*Present*
Ivan Pryvalov	Summer 2013–Summer 2014

Bachelor Thesis Student

Niklas Grimm	Winter 2012/13

TEACHING EXPERIENCE

Saarland University

Instructor, Advanced Course: Applied Cryptography	Winter 2014/15
Instructor, Seminar: Practical Cryptographic Systems	Winter 2012/13, Summer 2014
Co-Instructor, Advanced Course: Privacy Enhancing Technologies	Summer 2013, Summer 2014
Advisor, Seminar: Selected Topics in Information Security	Summer 2011

PROFESSIONAL ACTIVITIES

- Program Committee Member:
ProvSec 2015. FCS 2015. ICDCS 2015. ICWE 2015. CPSS 2015. ProvSec 2014. HotPETS 2014. WWW 2013. ACM WPES 2012.

- ◇ External Reviewer (Journals):
  ACM TISSec. Computer Security. Designs, Codes and Cryptography (DCC). IEEE TIFS. IEEE TDSC. Distributed Computing (DC). IEEE TPDS. IEEE Transactions on Computers (ToC). Information Processing Letters (IPL). Acta Informatica.
- ◇ Bitcoin Foundation Grant Committee 2014
- ◇ Centre for Applied Cryptographic Research (CACR) University of Waterloo
  Cryptography Seminar Organizer Spring 2008
- ◇ SecNet 2006, Annual Network Security Workshop IIT-Bombay
  Overall Coordinator Spring 2006

AWARDS AND GRANTS

- ◇ **Principal Investigator (joint)** for an Indo-German Max Planck Center for Computer Science (IMPECS) grant for "Identity-Based Cryptography and Beyond" 2014-17
- ◇ Nominated for a **Distinguished Dissertation Award** of the Canadian Association for Graduate Studies Winter 2011
- ◇ **University of Waterloo Graduate Scholarship** Winter 2008
- ◇ **David R. Cheriton Graduate Scholarship**, University of Waterloo 2007–10
- ◇ **Technical Color** for excellence in technical activities by Computer Science and Engineering Association (CSEA), IIT-Bombay 2005–06
- ◇ Competence in Software Technology **(CST) award** by the Centre for Development of Advanced Computing (C-DAC), India 2004

OTHER SERVICES AND WORK

- ◇ Research Group Leaders' Representative at the MMCI Clusterboard, Saarland University 2013-15
- ◇ Director Search Committee, School of Computer Science University of Waterloo
  Graduate Students Representative 2009-10
- ◇ Division Manager (Don) at Waterloo Co-op Residence Inc.(WCRI), Canada Fall 2008
- ◇ Member of Technical Staff, Persistent Systems Pvt. Ltd. (PSPL), India Mar 2004–Jul 2004
- ◇ Trainee System Analyst, National Stock Exchange (NSE.iT), India Aug 2003–Mar 2004

BIOGRAPHICAL INFORMATION

I am an Indian citizen and a Canadian permanent resident. I speak fluent English, and native Hindi and Marathi. I have been learning German recently.

ACADEMIC REFERENCES

The following people can be contacted to provide references about my academic work.

Ian Goldberg
School of Computer Science
University of Waterloo
200 University Avenue West
Waterloo, Canada. N2L 3G1
iang@cs.uwaterloo.ca

Michael Backes
Computer Science
Saarland University
Campus E1 1
Saarbruecken, Germany 66123
backes@cs.uni-saarland.de

Peter Druschel
Distributed Systems Group
MPI-SWS
Campus E1 5
Saarbruecken, Germany 66123
druschel@mpi-sws.org

Nikita Borisov
Electrical & Computer Engineering
UIUC
1308 West Main Street
Urbana, IL, USA 61801?2307
nikita@illinois.edu

Amir Herzberg
Computer Science
Bar-Ilan University
Room 10, Building 408
52900 Ramat-Gan, Israel
herzbea@cs.biu.ac.il

Alfred Menezes
Combinatorics & Optimization
University of Waterloo
200 University Avenue West
Waterloo, Canada. N2L 3G1
ajmeneze@uwaterloo.ca

Aniket Kate
Jan 2014