

Amrit KUMAR

PERSONAL DATA

DATE OF BIRTH: 4 December 1988
NATIONALITY: Indian
ADDRESS: 2 Avenue des Jeux Olympiques, Grenoble, France
PHONE: +33 674 955 994
EMAIL: amrit.kumar@polytechnique.org
WEBPAGE: privatics.inrialpes.fr/~amkumar

RESEARCH INTERESTS

Applied Cryptography: secure outsourcing of computations, secure multi-party protocols; Security and Privacy issues in the web.

EDUCATION

<i>Current</i> Nov 2013	PhD in Computer Science Université Grenoble Alpes and Privatics team, Institut National de Recherche en Informatique et en Automatique (INRIA), France THESIS: <i>Secure and Private Information Outsourcing</i> ADVISORS: Cédric Lauradoux and Pascal Lafourcade Supported by the Labex PERSYVAL-LAB (ANR-11-LABX-0025-01) funded by the French program Investissement d'avenir.
2012-2013	Masters in Security, Cryptology and Coding of Information Systems École Nationale Supérieure d'Informatique et Mathématiques Appliquées de Grenoble (ENSIMAG), France Double degree with École Polytechnique, France.
2009-2012	Engineer Diploma École Polytechnique, Palaiseau, France Major in Computer Science with specialization in <i>Algorithm and Optimization</i> .
2006-2009	Bachelor of Science Presidency College, University of Calcutta, India Major in Mathematics with Physics and Chemistry as ancillary subjects <i>First Class Honors</i> .

WORK EXPERIENCE

MAY-AUG 2016	Visiting researcher at University of Calgary, Canada THESIS: <i>Secure Outsourcing of Storage and Computation</i> ADVISOR: Reihaneh Safavi-Naini
JUN-SEP 2013	Research internship at INRIA Grenoble, MOAIS team THESIS: <i>Trusted Sky and Cloud Computing</i> ADVISORS: Jean-Louis Roch and Clément Pernet
APR-JUN 2012	Research internship at INRIA Rennes, CELTIQUE team THESIS: <i>Proofs as Cryptography: a new interpretation of the Curry-Howard isomorphism for software certificates</i> ADVISORS: Pierre-Alain Fouque and Thomas Genet
APR 2011	Industrial internship at MICHELIN, Clermont-Ferrand, France In the planning and optimization team at tyre retreading site of Combaude.

SCHOLARSHIPS AND AWARDS

2015	MITACS Globalink Research Award - INRIA For a research internship at University of Calgary.
2012-2013	Masters' Excellence Scholarship Persyval-Labex grant, Grenoble.
2012-2013	Grenoble Institute of Technology Foundation Scholarship Scholarship for master-level studies at ENSIMAG.
2009-2012	École Polytechnique's Foundation Scholarship Scholarship for engineering studies at École Polytechnique.
2005	KVPY Fellow A scholarship program of Dept. of Science & Technology, Govt. of India, run and managed by Indian Institute of Science, Bangalore.
2005	National Initiative on Undergraduate Science (NIUS) Fellow A fellowship program of Dept. of Science & Technology, Govt. of India, run and managed by Tata Institute of Fundamental Research, Mumbai.

TEACHING EXPERIENCE

FEB-MAY 2015	ENSIMAG
FEB-MAY 2014	COURSE: <i>Coding and Security of Networks</i>
FEB-APR 2013	RESPONSIBILITIES: Teaching assistance for lab sessions Level: Graduate Language: French Volume: 24h
SEP-DEC 2015	ENSIMAG
SEP-DEC 2014	COURSE: <i>Algorithm and Discrete Optimization</i> RESPONSIBILITIES: Lecturing and teaching assistance Level: Graduate Language: French Volume: 80h
SEP-JAN 2015	ENSIMAG
SEP-JAN 2014	COURSE: <i>Security Models in Cryptography</i> RESPONSIBILITIES: Teaching assistance for exercise sessions Level: Graduate Language: English Volume: 18h
JUN-NOV 2013	Scientific tutoring at Université Joseph Fourier RESPONSIBILITIES: Tutoring a graduate student in Computer Science
AUG-SEP 2011	English tutoring at École Polytechnique RESPONSIBILITIES: English tutoring lessons to undergraduate students

INTERNSHIP SUPERVISIONS

FEB-JUN 2015	Lenka Kuníknová, ENSIMAG Level: Graduate With Cédric Lauradoux THESIS: <i>An Efficient Implementation of a Generic two-party Secure Computation Protocol in the UC Framework</i>
NOV-JUN 2015	Jonathan Tournier, Université Joseph Fourier Level: Graduate With Cédric Lauradoux THESIS: <i>Evaluating the Security of Forensic Tools</i>
NOV-JUN 2013	Elie Duleu, ENSIMAG Level: Undergraduate With Jean-Louis Roch THESIS: <i>Algorithm-Based Fault Tolerant Outsourcing of Matrix Computations</i>
NOV-JUN 2013	Thomas Gerbet, Université Joseph Fourier Level: Graduate With Cédric Lauradoux THESIS: <i>New Denial-of-Service Attacks on Non-cryptographic Hash Function based Primitives</i>

REVIEWING SERVICE

CONFERENCE: DISC'14, CCSW'14, WiSec'14, CSS'14, FPS'14, FPS'15, RESSI'16

JOURNAL: TISSEC

CONFERENCE PUBLICATIONS

- [1] Thomas Gerbet, Amrit Kumar, and Cédric Lauradoux. A Privacy Analysis of Google and Yandex Safe Browsing. In *46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2016, Toulouse, France, June 25-July 1, 2016*.
- [2] Thomas Gerbet, Amrit Kumar, and Cédric Lauradoux. The Power of Evil Choices in Bloom Filters. In *45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2015, Rio de Janeiro, Brazil, June 22-25, 2015*.
- [3] Amrit Kumar and Cédric Lauradoux. A Survey of Alerting Websites: Risks and Solutions. In *ICT Systems Security and Privacy Protection - 30th IFIP TC 11 International Conference, SEC 2015, Hamburg, Germany, May 26-28, 2015*.
- [4] Amrit Kumar, Pascal Lafourcade, and Cédric Lauradoux. Short Paper: Performances of cryptographic accumulators. In *39th IEEE Conference on Local Computer Networks, LCN 2014, Edmonton, AB, Canada, 8-11 September, 2014, 2014*.
- [5] Amrit Kumar and Cédric Lauradoux. Private Password Auditing - Short Paper. In *Technology and Practice of Passwords - International Conference on Passwords, PASSWORDS'14, Trondheim, Norway, December 8-10, 2014, Revised Selected Papers, 2014*.

RESEARCH REPORTS

- [1] Thomas Gerbet, Amrit Kumar, and Cédric Lauradoux. (Un)Safe Browsing. Research Report RR-8594, INRIA, September 2014. <https://hal.inria.fr/hal-01064822/>.
- [2] Amrit Kumar, Pierre-Alain Fouque, Thomas Genet, and Mehdi Tibouchi. Proofs as Cryptography: A New Interpretation of the Curry-Howard Isomorphism for Software Certificates. *HAL*, hal-00715726, 2012. <http://hal.archives-ouvertes.fr/hal-00715726/>.

OTHERS (PEER-REVIEWED)

- [1] Amrit Kumar and Cédric Lauradoux. New Dimensions in Phishing. In *5ème Atelier sur la Protection de la Vie Privée (APVP)*, Cabourg, France, June 2014.
- [2] Amrit Kumar and Jean-Louis Roch. Algorithm-Based Secure and Fault Tolerant Outsourcing of Matrix Computations. In *Information Hiding and Interactions with Codes and Cryptography Days*, Paris, France, October 2013. Extended Abstract: <http://hal.archives-ouvertes.fr/hal-00876156>.
- [3] Amrit Kumar, Jean-Louis Roch, and Clément Pernet. Fast Abstract: Secured Outsourced Linear Algebra. In *SAFECOMP'2013, The 32nd International Conference on Computer Safety, Reliability and Security*, Toulouse, France, August 2013. Extended Abstract: <http://hal.inria.fr/hal-00926723>.

PROGRAMMING SKILLS

SOFTWARE: SCILAB, OCTAVE, SAGE, PARI/GP
PROGRAMMING C, PERL, JAVA, PYTHON, OCAML
LANGUAGES:
OTHERS: HTML, PHP, JAVASCRIPT, SQL

LANGUAGES

HINDI: Mother tongue
ENGLISH: Fluent, TOEFL ibt score-106 (Taken in 2011)
FRENCH: Fluent, TCF: level B2 (Taken in 2012)
CHINESE: Beginner