Charles Phelps Taft Research Center

at the University of Cincinnati

Conferences and Lectures

Competitive Lecture Grant Application

Each section (I-III) should be placed at the start of a new page. All required documents must be included in a single document, uploaded to the electronic submissions system, no later than 5PM on the published day of the deadline. Intradepartmental review is required for most programs and applicants should plan the timing of their submission accordingly. Taft does not accept an obligation to review applications that have not received intradepartmental review by the time the committee convenes.

I. General Information

a. Sponsoring Department(s): Mathematics and Political Sciences

b. Individual sponsor: Jintai Ding and Richard Harknett

c. Name of Lecturer: Johannes Buchmann

d. Institutional Affiliation: Technical University of Darmstadt

e. If the lecturer is International Speaker, list visa type:

f. Lecture Title: A Multidisciplinary Approach to Internet Privacy

g. Date, Time, and Location of Lecture: 4-5pm, September 5, 2013, Taft House

II. Budget

a. Transportation: 1300

b. Lodging: 500

c. Honorarium: 2500

d. Have you already applied (or will you in the future) for other grants for this travel, including departmental support? No

e. Is this request for a departmental speaker? If yes, please indicate what remains of departmental lecture fund and what will be committed to this engagement? No.

f. Total Amount Requested from the Competitive Lecture Fund: 4300

III. Lecture Details

a. Brief, general description of lecture content:

b. Lecture Rationale

c. Please outline the intended activities (i.e. conference lecture, public lecture, round-table discussion, etc) and audience (size, composition).

d. Short description of speaker:

e. Please supply a brief description of the proposed speaker's work and reputation along with a short C.V.

Proposal for Taft Competitive Lecture

Jintai Ding, Richard Harknett

1 Name of speaker, lecture title, and date of lecture

Name of Lecturer: Professor Johannes Buchmann

Institutional affiliation: Technical University of Darmstadt

Title of Lecture(s): A Multidisciplinary Approach to Internet Privacy

Date and time of Lecture (Lectures held at Taft House unless otherwise noted): 4-5pm, September 5, 2013

2 Speaker and Lecture description

Johannes Buchmann is a world leading expert in the area of information security. His main research area is in the field of theoretical computer science - cryptography and computer algebra, in particular, cryptography. He made fundamental contributions in the design of new algorithms in algebraic number theory, the design of new cryptographic techniques and the use of cryptographic techniques in practice. He is a director and one of the main founders of the Center for Advanced Security Research Darmstadt (CASED) at Technical University of Darmstadt, one of the strongest research centers in information security in the world. From 2002 to 2007 he was Vice-President for Research at the TU Darmstadt and he is a member of German Academy of Sciences.

As we are now moving into an information-based society, privacy, in particular, Internet privacy becomes an increasing concern from the perspective of individual rights and overall well-being of our society. Internet privacy involves the right of an individual's personal privacy concerning the storing, reusing, third-party accessing, and displaying of information pertaining to the individual via the Internet. Privacy include either Personally Identifying Information (PII) or non-PII information such as a website visitor's behavior. PII refers to any information that can be used to identify an individual, such as name, age, physical address and medical information like DNA. In our current technological world, millions of individuals are subject to Internet privacy threats.

In the last few years, Professor Johaness Buchmman led a team of researchers working on a project "Internet Privacy" funded by German federal government. The goal of the interdisciplinary project Internet-Privacy, is to develop recommendations (including prototypes), for business, economy, science and academia that promote a culture of privacy and promote trust in Internet applications and data transmissions. These recommendations will be applied to legal matters, education, business ethics and research demands.

This project involves academic professionals from the fields of Ethics, Sociology, Law, Economics, and Mathematics, Computer science and other technical areas. The research group developed proposals for social rules and norms, an economic and legal framework, and suggested technical solutions. These proposals demonstrate how an adequate measure of privacy can be evaluated and implemented in the context of various Internet user including Web 2.0 (including social networks) and e-Commerce. They recently published the volume I of the study (328 pages) "Internet Privacy - A Culture of Privacy and Trust for the Internet" and a technical report titled "Technical Aspects of Online Privacy". The technical report gives an overview of the state of the art, the major problems and identifies technical solutions to the problems. The report includes an in-depth analysis of social networks like Facebook. These works have attract attentions all around the world.

Professor Buchmann is invited to deliver the lecture to present the main findings of their results in the project "Internet Privacy" based on their innovative multidisciplinary approach.

3 Rationale

The rationale for inviting Professor Buchmann to give the prestigious Taft Lecture comes from several directions. One is that Dr. J. Ding have been developing a strong cryptography group at the Department of Mathematical Sciences and they are very interested in expanding into new research directions in the area of Internet privacy protection using cryptography and they have been developing some new ideas in this area using lattice-based cryptosystems, in particular, the solutions which are based on new Identity-based encryption technology they have been developing in the last two years. Dr. R. Harknett on the other hand have been making significant progresses in the area of information security from the perfective of policy. Dr. Harknett is also very interested in expanding into the area of policy concerning Internet privacy. Dr. Ding and Dr, Harknett both are involved in developing a new interdisciplinary program in information security at UC and privacy will be one of the main focus areas. We believe the lecture of Professor Buchmann is a very good way to expose the cutting edge research in information security to the general audience at UC where there are tremendous interests from various areas. This lecture could work as a catalyst to attract people from all areas to work on the new interdisciplinary program in information security at UC. This Taft lecture is intended for a broad audience including students, researchers, professors and people from industry and government. Clearly such a lecture fits well with the general goal of the UC2019 plan.

4 An outline of the intended activities

We plan to have an one hour public lecture and afterwards we plan to have a discussion session (around 30 minutes) on the impact of Internet privacy on the the future on our society and how we can deal with the related problems with a multidisciplinary approach. We expect a large audience from all around the university and we expect at least 100 to be at the lecture. This audience should include students and faculties from various department such as mathematics, computer science, computer engineering, electric engineering, law, business, sociology, psychology and many other areas. We plan to have the speaker to give one more technical discussion lecture in the form of a seminar. This will be devoted to explaining in more technical details how we can technically deal with the problem of Internet privacy, how the tools could be designed and how to analyze their effectiveness. The seminar audience should include graduate students and faculties from all areas as well but mainly from mathematics, computer sciences, political sciences, sociology, and psychology. We expect to have about 10 faculties and 20 graduate students. Further discussions with students and faculties will also be arranged.

5 Budget Rationale

Air travel and local travel: 1300 $

Four nights hotel: 500$

The honoraria: 2500$. The disciplinary norms for people in information security is much higher normally than in mathematics, this amount is in a middle spectrum within the area of information security for the speaker with similar status.

Total: 4300 $

The departmental Taft money for 2012 in both Mathematics and Political Sciences is already completely committed to other speakers and no more money is available. Since this is a very interdisciplinary-multidisciplinary lecture, we do not expect to have any departmental Taft money support for this lecture

Johannes Buchmann Ph.D.

CONTACT INFORMATION

Professor fur Informatik und Mathematik
Technische Universitat Darmstadt
Fachbereich Informatik
Hochschulstrasse 10
64289 Darmstadt, Germany

EDUCATION

1974 - 1979, Study of mathematics, physics, philosophy and pedagogy at the University of Cologne, Germany
1979, Erste Staatsprfung fr das Lehramt an Gymnasien equivalent of master degree
1980 - 1983, Research assistant at the University of Cologne
1982, Doctorate in Mathematics at the University of Cologne (Supervisor Prof. Dr. Hans-Joachim Stender)

WORK EXPERIENCES

1984 - 1985, Research assistant at the University of Cologne
1985 - 1986, Feodor-Lynen research fellow of the Alexander von Humboldt-Stiftung at the Ohio State University (Advisor: Prof. Dr. Hans Zassenhaus)
1985 - 1986, Research assistant at the University of Dsseldorf
1988, Habilitation in Mathematics at University Dsseldorf (Advisor: Prof. Dr. Michael Pohst)
1988 - 1996, Professor of Computer Science at the Universitat des Saarlandes, Germany
1996 - Professor of Computer Science and Mathematics at Technische Universitat Darmstadt Germany
1996, Member of Academy of Sciences and Literature Mainz
2000, Co-founder of FlexSecure GmbH
2001 - 2007, Vice President for Research at the Technical University of Darmstadt
2003 - Chairman of CAST - Competence Center for Applied Security Technology, Darmstadt e.V.
2006, Member of Berlin-Brandenburg Academy of Sciences
2006, Honory Doctorate of the University Debrecen, Hungary
2008, Charles Phelps Taft Research Center Visiting Fellow, University of Cincinnati
2008, Member of German Academy of Science and Engineering acatech
2008 - 2011, Director of the Center for Advanced Security Research Darmstadt CASED
2011 - Vice-Director of the Center for Advanced Security Research Darmstadt CASED
2011, Member of German Academy of Sciences Leopoldina

HONORS AND AWARDS

1993 Gottfried Wilhelm Leibniz Prize (together with Claus-Peter Schnorr), for his work on the algorithmic number theory and cryptography
2003 Innovation Award of the State of Hesse
2006 Karl Heinz Beckurts Award for his work at the computer security by using electronic signatures
2008 IT Security Award of the Horst Gortz Foundation (2nd place, with Erik Dahmen)
2012 Tsungming Tu Prize of National Science Council Taiwan

TEACHING

More than 220 Bachelor-, Master- und Diplomatheses supervised 57 PhD Theses supervised

ACADEMIC SERVICES

Member of the Editorial Board Journal of Cryptology 1990 - 2009

Editorial Board for Discrete Mathematics, International Journal of Mathematics and Computer Science, Teubner Texte zur Informatik, Encyclopaedia of Mathematical Sciences: Number Theory, Industrial Mathematics

Speaker of the Graduate School, Departement of Computer Science, Saarland University 1990-1996

Chairman of the Department of Computer Science, Saarland University 1993-1995

Dean (Study) of the Department of Computer Science, TU Darmstadt 2000 - 2001

Vice President of the TU Darmstadt 2001-2007

Reviewer for DFG-Einzelantr?ge, Forschergruppen, Sonderforschungsbereiche ,National Sience Foundation, US, National Sience and Engeneering Research Council, Canada, Schweizer Nationalfond

Member advisory board for the "Research center for applied cryptography", University of Waterloo

Member of Technical Advisory Panel of Center for Information Security and Cryptography Calgary

Member of Trustees of the Fraunhofer Institute SIT

Member of Federal Scientific Advisory Board of the Federal