UNIVERSITY OF MARYLAND

2123 Lee Building
College Park, Maryland 20742-5121
301.405-0281 TEL 301.314.9305 FAX
Email: gradtravelawards@umd.edu

Application for the Jacob K. Goldhaber Travel Award

For graduate student participation at an academic conference

Contact Information

Qian — Yi
Last (please complete above) — First — M.I.

3270 A.W. Williams
Address (campus address preferred; include building name & room #)

College Park — MD — 20740
City — State — Zip

yiqian@umd.edu — 111351282
UMD Email address — Student Identification Number/UID

Conference Dates

Conference begins: 11/03/2014

Conference ends: 11/07/2014

Have you received a Goldhaber award before?

Yes (No)

If yes, what date ? _____

Conference Information

21st ACM Conference on Computer and Communication Security
Name of Conference

Streaming Authenticated Data Structures: Abstraction and Implementation
Title of Presentation

The Scottsdale Plaza Resort, Scottsdale, Arizona, USA
Location of Conference

Education

CMSC
Department Code (e.g., CHEM)

PhD
Degree Sought

If PhD, have you advanced to candidacy?
___Yes X No

Advisor's Name

Itemized Budget

Transportation $	650
Registration fees $	300
Lodging $	350
Food $	200
Other $	
Specify Other	
Total Est. Budget $	1500
Amount requested $ from Goldhaber	400

Graduate School Use Only

Application Received:

Award Amount:

Revised 2014

Materials and Signature

✓ Application
✓ Copy of Conference Invitation
✓ Advisor's Letter
✓ Abstract / Proposal

Your signature below indicates acceptance of the guidelines found on the Graduate School website and verifies that all the information is complete and accurate. Incomplete applications will not be considered for funding.

Yi Qian
Applicant's signature

10/07/2014
Date (mm/dd/yy)

All Funding and Funding Sources

(KFS account # and funding amount)

1. 434330 - $500
2.
3.
4.

Jeffrey Foster
Print name of Funding Representative
(Dean, Chair, Grad Dir, or external source)

Jeffrey Foster
Signature of Funding Representative

Graduate Director
Title of Funding Representative

10/7/14
Date

Dear Author,

Your submission, "Streaming Authenticated Data Structures: Abstraction and Implementation" was accepted for publication in CCSW'14 conference proceedings. You must formally grant permission to ACM to publish this contribution before ACM can proceed with production.

There are several ways you may now assign publishing rights to ACM. You may ask ACM to manage your rights for you (including pursuit of plagiarism and clearance of third-party re-use permissions) by transferring the requested rights to ACM using either the traditional ACM Copyright Transfer Agreement or the ACM Publishing License.

The community has also asked ACM to offer up-front OA fees should authors wish to make their works permanently open access (OA) in the ACM Digital Library.

Should you choose to pay the article fee guaranteeing permanent open access, you may still ask ACM to manage your publishing rights for you by copyright or license. But you will also have a third option: you may choose to manage all rights yourself, by selecting the Permission Form, granting ACM a non-exclusive permission to publish your work.

As of April 2013, ACM is offering authors the option of paying an Article Processing Charge in exchange for permanent OA (open access) for your article in the ACM Digital Library. Should you choose to pay the article fee guaranteeing permanent open access, you may still ask ACM to manage your publishing rights for you (including pursuit of plagiarism and allowing ACM to grant re-use permissions) by transferring the requested rights to ACM using either the traditional ACM Copyright Transfer Agreement or the ACM Publishing License. But you also have a third option: you may choose to manage all rights yourself, by selecting the Permission Form, granting ACM a non-exclusive permission to publish your work.

The Open Access option requires the payment of the APC (Article Processing Charge). The fee is $900 if you are not a member of ACM or $700 if you or any of your co-authors are ACM members. If you choose the Open Access option, ACM will invoice you separately. If you are not already a member of ACM, consider joining ACM now to take advantage of the member discount rate http://campus.acm.org/public/qj/quickjoin/interim.cfm?promo=PROSOA.

If you do not want to pay the OA fee, you will need to transfer publishing rights to ACM either by using the traditional ACM Copyright Transfer Agreement or choosing the new ACM Publishing License.

Please click on the following link to access and complete the required process of choosing publishing rights for your submission.

http://cms.acm.org/oa.cfm?confID=020500041C0309070405&proceedingID=06000106&paperID=09&sequence=1

Please take a moment to review the form above for errors in the title and author listing. If corrections are needed, please PROCEED to the selected FORM and use the EDIT/tool function located at top of the form and make any necessary changes before submitting the form. The changes will automatically be sent to the PC or proceedings coordinator upon completion. We request that you attend to and complete the form above within 72 hours of the sending of this email.

If the link above does not contain your paper's information, please contact me at your earliest convenience.

Here is additional information about the difference between the forms: http://authors.acm.org. The FAQ tab is particularly helpful.

Deborah Cotton
ACM Publications
rightsreview@acm.org

encompasses CCSW), **4 of the top 20 cited papers of the past five years come from CCSW**. One way to look at it is that you're as likely or perhaps more likely to have a top-20 paper publishing in CCSW than in CCS! (thanks to Ari Juels for noticing this)

Student Stipends

Student stipends may be available to attend CCSW. Please apply on the CCS website for a CCS grant and then email radu@digitalpiglet.org to let us know why you would be a good fit for CCSW. We plan on awarding **several student travel grants** (a function also of the quality of the applications).

Important Dates

Submissions due: **30 July, 2014 (midnight anywhere in the world)** (absolutely firm)
Author notification: **25 August, 2014**
Camera-ready: **7 September, 2014**
Workshop: **November 7, 2014**

Submissions

CCSW is soliciting full papers of up to 12 pages which will be judged based on the quality per page. Thus, shorter, high-quality papers are encouraged, and papers may be perceived as too long if they are repetitive or verbose. Submissions must use the ACM SIG Proceedings Templates (available at the ACM website) in double-column format with a font no smaller than 9 point. Only PDF files will be accepted. Submissions not meeting these guidelines risk rejection without consideration of their merits. Accepted papers will be published by the ACM Press and/or the ACM Digital Library.

Submissions must be anonymous, and authors should refer to their previous work in the third-person. Submissions must not substantially overlap with papers that have been published or that are simultaneously submitted to a journal or a conference with proceedings. Each accepted paper must be presented by one registered author. Submissions not meeting these guidelines risk immediate rejection. For questions about these policies, please contact the chairs.

Please submit your paper via EasyChair.

Keynote Speakers

users with only 30 software engineers. These building blocks demonstrate the power of cloud computing and have fundamentally changed how applications will be created and delivered in the future. Unfortunately, fitting security into this picture -- at the application or the infrastructure level -- remains a tremendous challenge. It doesn't need to be this way. With an aggressive research investment, we can reduce the cost of high quality security. This talk will explore why security is so expensive and what can be done to reduce this cost, from the perspective of someone working to create security focused cloud infrastructure while also leading security efforts in the OpenStack community.

10:30 - 11:00 **Coffee Break**

Session: Secure computation **Chair: TBD**

11:00 - 12:00 **A Framework for Outsourcing of Secure Computation**
Jesper Buus Nielsen; Claudio Orlandi

Certification and Efficient Proofs of Topology Graphs
Thomas Gross

Streaming Authenticated Data Structures: Abstraction and Implementation
Yi Qian, Yupeng Zhang, Xi Chen and Charalampos Papamanthou

Keynote II

12:00 - 12:50 **Privacy vs. Efficacy in Cloud-based Threat Detection**, David Mc Grew (Fellow, Cisco)
Abstract: Advanced threats can be detected by monitoring information systems and networks, then applying advanced analytic techniques to the data thus gathered. It is natural to gather, store, and analyze this data in the Cloud, but doing so introduces significant privacy concerns. There are technologies that can protect privacy to some extent, but these technologies reduce the efficacy of threat analytics and forensics, and introduce computation and communication overhead. This talk considers the tension between privacy and efficacy in Cloud threat detection, and analyzes both pragmatic techniques such as data anonymization via deterministic encryption and differential privacy as well as interactive techniques such as private set intersection and searchable encryption, and highlights areas where further research is needed.

12:50 - 14:00 **Lunch**

Session: Storage security **Chair: TBD**

14:00 - 14:40 **Reconciling End-to-End Confidentiality and Data Reduction In Cloud Storage**
Nathalie Baracaldo; Elli Androulaki; Joseph Glider; Alessandro Sorniotti

Abstract

In the setting of streaming verifiable computation, a verifier and a prover observe a stream of n elements $x_1, x_2, \ldots, x_n$ and later, the verifier can delegate a computation (e.g., a range search query) to the untrusted prover over the stream. The prover returns the result of the computation and a cryptographic proof for its correctness. To verify the prover's result efficiently, the verifier keeps small local (logarithmic) state, which he updates while observing the stream. The challenge is to enable the verifier to update his local state with no interaction with the prover, while ensuring the prover can compute proofs efficiently.

Papamanthou et al. (EUROCRYPT 2013) introduced *streaming authenticated data structures* (SADS) to address the above problem. Yet their scheme is complex to describe and impractical to implement, mainly due to the use of Ajtai's lattice-based hash function. In this work we present an *abstract* SADS construction that can use any hash function satisfying properties that we formally define. This leads to a *simpler* exposition of the fundamental ideas of Papamanthou et al.'s work and to a *practical* implementation of a streaming authenticated data structure that employs the efficient SWIFFT hash function, which we show to comply with our abstraction. We implement both the EUROCRYPT 2013 construction and our new scheme and report major savings in prover time and public key size.

To whom it may concern,

It is my pleasure to recommend Yi Qian for the student travel fund offered by your prestigious program.

I began to know Yi when he took my graduate level course *Cloud Computing Security* at University of Maryland--College Park this spring. Yi first approached me to talk about the research project of the course. At our first meeting, I described the idea of replacing the hash function in my paper *Streaming Authenticated Data Structures* with a SWIFFT-like hash function to make the scheme more efficient. Thanks to his great effort, this course project accomplished more than the original goal and led to the paper *Streaming Authenticated Data Structures: Abstraction and Implementation,* which is accepted at CCSW 2014.

During the spring semester and the following summer, Yi demonstrated the ability to work independently with great creativity, confidence and enthusiasm. During our discussions, he asked good questions. He independently worked on the lattice-based new hash function, which is a theoretical problem with sophisticated mathematics involved. To my pleasant surprise, he also proposed an abstract framework for the original scheme, which leads to a better understanding and more insight. Clearly, Yi is very comfortable with math and has a deep understanding of CS notions.

Yi excels in explaining his ideas, and has shown good communication skills, too. The other two students favorably commented about working with Yi. He showed great willingness to compromise with other research partners. I think they form a good team, and look forward to future collaborations among them.

It would be the first time for Yi to attend CCSW and present his paper this November. There is no doubt that this would be a great opportunity for him as a young researcher. As a first year faculty member, however, I have not yet secured funding from external sources. He will need financial support to make the trip.

Sincerely,

Charalampos (Babis) Papamanthou
09/09/2014