PETER RINDAL

521 NW 14th St, Corvallis, OR 97330 | (509) 520-8701 | rindalp@oregonstate.edu
web.engr.oregonstate.edu/~rindalp

SUMMARY

I am a PhD student at Oregon State University studying cryptography with special interest in the field of secure multi-party computation and its applications. My career goal is to invent privacy enhancing technologies that can meet real world constraints.

PUBLICATIONS

Improved Private Set Intersection against Malicious Adversaries

- Private set intersection (PSI) refers to a special case of secure two-party computation in which the parties each have a set of items and compute the intersection of these sets without revealing any additional information. In this paper we present improvements to practical PSI providing security in the presence of malicious adversaries.

Secure Data Exchange: A Marketplace in the Cloud

- We describe a protocol called Secure Data Exchange, where several data owners are storing private encrypted data in a semi-honest non-colluding cloud, and an evaluator (a third party) wishes to engage in a secure function evaluation on the data belonging to some subset of the data owners. Our protocol ensures that none of the parties involved learns anything beyond what they already know and what is revealed by the function output, even when the parties (except the cloud) are actively malicious.

Faster Malicious 2-party Secure Computation with Online/Offline Dual Execution

- Designed a highly optimized protocol for general-purpose secure two-party computation in the presence of malicious adversaries. Our starting point is a protocol of Kolesnikov et al. (TCC 2015). We adapt that protocol to the offline/online batched-execution setting. Our implementation of the protocol achieved the fastest running times to date of 2ms online and 5ms amortized offline when evaluating the AES circuit.

EXPERIENCE

Jan. 2016 – Sept. 2016 Research Intern, *Microsoft Research*

- Developed the Secure Data Exchange (SDE) protocol and implementation along with several applications which demonstrate how economic incentives can be aligned to make the SDE have a viable business model. During a follow-up internship, a special purpose protocol for training machine learning models based on the boosted decision tree algorithm was designed and implemented.

July 2014 – Dec. 2014 Software Engineer Intern, *Digimarc*

- Worked in a medium size development team on a variety of projects ranging from image processing, API design, and software security.

EDUCATION

Oct. 2010 – July 2014 Bachelors of science Degree, Computer Science, *Oregon State University*

3.6 Cumulative GPA
3.76 Computer Science GPA

Jan. 2015 – exp. 2019 Doctor of Philosophy in the school of Computer Science, *Oregon State University*

3.9 Cumulative GPA

REFERENCES

Mike Rosulek	Principal Ph.D. Advisor	rosulekm@eecs.oregonstate.edu
Melissa Chase	Microsoft Research Mentor	melissac@microsoft.com
Attila Yavuz	Research Advisor	Attila.Yavuz@oregonstate.edu