PETER RINDAL

(509) · 520 · 8701 ◇ rindalp@OregonState.edu
1445 NW Vista Pl. ◇ Corvallis, OR 97330
`web.engr.OregonState.edu/~rindalp`

EDUCATION

Ph.D. in Computer Science *January 2015 — Est. June 2019*
Oregon State University, Corvallis
Overall GPA: 3.9

B.S. in Computer Science *September 2010 — June 2014*
Oregon State University, Corvallis
Overall GPA: 3.65

RESEARCH INTERESTS

My primary interest is the development of efficient methods for computing on encrypted data. Most notably has been the development of a highly optimized protocol for performing general secure computation. I have also worked on Private Set Intersection for both malicious & semi-honest adversaries, and several projects combining machine learning, differential privacy and secure computation.

EMPLOYMENT

Oregon State University January 2015 — present
Graduate Research Assistant Corvallis, OR

Visa Research June 2017 — September 2017
Security Research Intern Palo Alto, CA

Microsoft Research June 2016 — September 2016
Security Research Intern Redmond, WA

Microsoft Research January 2016 — March 2016
Security Research Intern Redmond, WA

Digimarc June 2014 — December 2014
Software Developer Intern Portland, OR

Boeing Company March 2013 — September 2013
Software Developer Intern Portland, OR

PUBLICATIONS

Note: the standard convention in this discipline is to list authors alphabetically.

Peer-reviewed conference publications:

C1 Peter Rindal and Mike Rosulek. *Faster Malicious 2-party Secure Computation with Online/Offline Dual Execution.* In *USENIX Security Symposium 2016.*

C2 Gizem Cetin, Hao Chen, Kim Laine, Kristin Lauter, Peter Rindal and Yuhou Xia. *Private Queries on Encrypted Genomic Data.* In *BMC Medical Genomics: iDASH Privacy and Security Workshop 2016.*

C3 Peter Rindal and Mike Rosulek. *Improved Private Set Intersection against Malicious Adversaries.* In *EUROCRYPT: International Cryptology Conference 2017.*

C4 Hao Chen, Kim Laine and Peter Rindal. *Fast Private Set Intersection from Homomorphic Encryption.* In *CCS: ACM Conference on Computer and Communications Security 2017.*

C5 Peter Rindal and Mike Rosulek. *Malicious-Secure Private Set Intersection via Dual Execution.* In *CCS: ACM Conference on Computer and Communications Security 2017.*

Informal publications:

I1 Ran Gilad-Bachrach, Kim Laine, Kristin Lauter, Peter Rindal and Mike Rosulek. *Secure Data Exchange: A Marketplace in the Cloud.* In *IACR ePrint 2016.*

I2 Peter Rindal and Roberto Trifiletti. *SplitCommit: Implementing and Analyzing Homomorphic UC Commitments.* In *IACR ePrint 2017.*

I3 Melissa Chase, Ran Gilad-Bachrach, Kim Laine, Kristin Lauter and Peter Rindal. *Private Collaborative Neural Network Learning.* In *IACR ePrint 2017.*

PRESENTATIONS

Conference and workshop presentations:

P1 *Faster Malicious 2-party Secure Computation with Online/Offline Dual Execution.* Usenix Security 2016, Austin Texas, USA, August 2016.

P2 *Improved Private Set Intersection against Malicious Adversaries.*

- Eurocrypt, Paris, France, April 2017.
- Theory and Practice of Secure Multiparty Computation, Bristol UK, April 2017.

Other invited talks:

T1 *A Survey of Oblivious RAM Methods and Optimizations.* Intel seminar, Hillsboro OR, USA, March 2015.

SOFTWARE PROJECTS

S1 Peter Rindal. *libOTe: A fast, portable, and easy to use Oblivious Transfer Library.*

S2 Peter Rindal. *Ivory-Runtime: A generic Secure Computation API for garbled circuits, SPDZ, etc.*

S3 Peter Rindal and Ni Ni Triue. *libPSI: A library for malicious and semi-honest Private Set Intersection (PSI).*

S4 Peter Rindal and Roberto Trifiletti. *SplitCommit: A portable C++ implementation of the [FJNT16] XOR-homomorphic commitment scheme.*

S5 Peter Rindal. *Batch Dual Execution: Malicious secure online/offline MPC implementation.*

SERVICE

External reviewer:

E1 *15th Theory of Cryptography Conference (TCC 2017).* Baltimore, MD, USA on November, 2017.

E2 *2nd IEEE European Symposium on Security and Privacy (EuroS&P 2017).* Paris, France on April, 2017.

E3 *19th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS 2017).* Boston, Massachusetts, USA on November, 2017.

REFERENCES

R1 Mike Rosulek, *Principle Ph.D. Advisor.* rosulekm@eecs.oregonstate.edu

R2 Payman Mohassel, *Microsoft Research Mentor.* pmohasse@visa.com

R3 Melissa Chase, *Microsoft Research Mentor.* melissac@microsoft.com