PETER RINDAL

(509) · 520 · 8701 ◇ PeterRindal@gmail.com
`ladnir.github.io`

EDUCATION

Ph.D. in Computer Science *January 2015 — Est. Sep. 2018*
Oregon State University, Corvallis
Overall GPA: 3.8

M.S. in Computer Science *January 2015 — Sep. 2017*
Oregon State University, Corvallis
Overall GPA: 3.8

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 highly optimized protocols for performing Private Set Intersection for both malicious & semi-honest adversaries. I have also worked on multi-party authenticated encryption, and several projects combining machine learning, differential privacy and secure computation.

EMPLOYMENT

Visa Research August 2018 — present
Staff Research Scientist San Francisco, CA

Oregon State University January 2015 — August 2018
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, Phillipp Schoppmann. *VOLE-PSI: Fast OPRF and Circuit-PSI from Vector-OLE.* In *EUROCRYPT: IACR International Cryptology Conference 2017.*

C2 – Saikrishna Badrinarayanan, Peihan Miao, Peter Rindal. *Multi-Party Threshold Private Set Intersection with Sublinear Communication.* In *PKC: Practice and Theory of Public-Key Cryptography 2021.*

C3 – Payman Mohassel, Peter Rindal and Mike Rosulek. *Fast Database Joins and PSI for Secret Shared Data.* In *CCS: ACM Conference on Computer and Communications Security 2020.*

C4 – Shashank Agrawal, Saikrishna Badrinarayanan, Pratyay Mukherjee, Peter Rindal. *Game-Set-MATCH: Using Mobile Devices for Seamless External-Facing Biometric Matching.* In *CCS: ACM Conference on Computer and Communications Security 2020.*

C5 – Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, Peter Rindal, Peter Scholl. *Efficient Two-Round OT Extension and Silent Non-Interactive Secure Computation.* In *CCS: ACM Conference on Computer and Communications Security 2019.*

C6 – Daniel Masny, Peter Rindal. *Endemic Oblivious Transfer.* In *CCS: ACM Conference on Computer and Communications Security 2019*

C7 – Adam Groce, Peter Rindal and Mike Rosulek. *Cheaper Private Set Intersection via Differentially Private Leakage.* In *PETS: Privacy Enhancing Technologies Symposium 2019.*

C8 – Daniel Demmler, Peter Rindal, Mike Rosulek and Ni Trieu. *PIR-PSI: Scaling Private Contact Discovery.* In *PETS: Privacy Enhancing Technologies Symposium 2018.*

C9 – Payman Mohassel and Peter Rindal. *ABY^3: A Mixed Protocol Framework for Machine Learning.* In *CCS: ACM Conference on Computer and Communications Security 2018.*

C10 – Shashank Agrawal, Payman Mohassel, Pratyay Mukherjee and Peter Rindal. *Threshold Authenticated Encryption.* In *CCS: ACM Conference on Computer and Communications Security 2018.*

C11 – Hao Chen, Kim Laine and Peter Rindal. *Labed-PSI: Improved Unbalanced Private Set Intersection with Fully Homomorphic Encryption.* In *CCS: ACM Conference on Computer and Communications Security 2018.*

C12 – Peter Rindal and Mike Rosulek. *Faster Malicious 2-party Secure Computation with Online/Offline Dual Execution.* In *USENIX Security Symposium 2016.*

C13 – 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.*

C14 – Peter Rindal and Mike Rosulek. *Improved Private Set Intersection against Malicious Adversaries.* In *EUROCRYPT: IACR International Cryptology Conference 2017.*

C15 – Hao Chen, Kim Laine and Peter Rindal. *Fast Private Set Intersection from Homomorphic Encryption.* In *CCS: ACM Conference on Computer and Communications Security 2017.*

C16 – 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.*

INVITED TALKS

T1 – *Privacy Preserving Machine Learning.* Arizona State University, Tempe AZ, USA, March 2021.

T2 – *Efficient Private Set Intersection from Homomorphic Encryption.* Simons Institute, UC Berkeley CA, USA, August 2020.

T3 – *Endemic Oblivious Transfer.* Sanford, Palo Alto CA, USA, August 2019.

T4 – *Improved Private Set Intersection.* Google, New York NY, USA, December 2017.

T5 – *Fast Private Set Intersection from Homomorphic Encryption.* MIT, Boston Massachusetts, December 2017.

T6 – *A Survey of Oblivious RAM Methods and Optimizations.* Intel seminar, Hillsboro OR, USA, March 2015.

SOFTWARE PROJECTS

S1 – Hao Chen, Kim Laine and Peter Rindal. *Asymmetric Private Set Intersection* (Microsoft).

S2 – Peter Rindal. *SMILY: Secure Multi-party Computation Library.* (Microsoft).

S3 – Peter Rindal. *ABY^3: A Mixed Protocol Framework for Machine Learning.* (Visa)

S4 – Peter Rindal. *Threshold Authenticated Encryption.* (Visa)

S5 – Peter Rindal. *Hydra: Threshold ECDSA.* (Visa)

S6 – Peter Rindal. *libOTe: A fast, portable, and easy to use Oblivious Transfer Library.* (Open Source) `https://github.com/osu-crypto/libOTe`. Includes the protocols of:

- Semi-honest 1-out-of-2 OT [IKNP03].
- Semi-honest 1-out-of-N OT [KKRT16].
- Malicious 1-out-of-2 OT [KOS15].
- Malicious 1-out-of-2 Delta-OT [KOS15],[BLNNOOSS15].
- Malicious 1-out-of-N OT [OOS16].
- Malicious approximate K-out-of-N OT [RR17].
- Malicious 1-out-of-2 base OT [NP00].

S7 – Peter Rindal. *Ivory-Runtime: A generic Secure Computation API for garbled circuits, SPDZ, etc.* (Open Source) `https://github.com/ladnir/Ivory-Runtime`. Includes the protocols of:

- Semi-honest 2PC [Yao82],[ZRE14].
- Semi-honest 3PC [FLNW16].

S8 – Peter Rindal and Ni Ni Triue. *libPSI: A library for malicious and semi-honest Private Set Intersection.* (Open Source) `https://github.com/osu-crypto/libPSI`. Includes the protocols of:

- Semi-honest Bloom filter PSI [DCW10].
- Semi-honest cuckoo hashing PSI [KKRT16].

- Malicious Bloom filter PSI [RR17a].
- Malicious public key crypto PSI [DKT10].
- Malicious cuckoo hashing PSI [RR17b].
- Semi-honest PIR [BGI16].

S9 – Peter Rindal and Roberto Trifiletti. *SplitCommit: A portable C++ implementation of the [FJNT16] XOR-homomorphic commitment scheme.* (Open Source) `https://github.com/AarhusCrypto/SplitCommit`

S10 – Peter Rindal. *Batch Dual Execution: Malicious secure online/offline MPC implementation.* (Open Source) `https://github.com/osu-crypto/batchDualEx`

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.

E4 – *18th International Conference on Cryptology in India (Indocrypt 2017).* Chennai India on December 2017.

E5 – *39th IEEE Symposium on Security and Privacy (S&P 2018).* San Francisco California, USA on May 2018.

E6 – *21st edition of the International Conference on Practice and Theory of Public Key Cryptography (PKC 2018).* Rio De Janeiro, Brazi on March 2018.

E7 – *38th International Cryptology Conference (Crypto 2018).* Santa Barbara California, USA on August 2018.

E8 – *DBSec 2018 : 32nd IFIP WG 11.3 Conference on Data and Applications Security and Privacy.* Bergamo, Italy on July 2018.

REFERENCES

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

R2 – Payman Mohassel, *Visa Research Manager. Now at Facebook.* payman.mohassel@gmail.com

R3 – Hoe Chen, *Microsoft Research Coworker. Now at Facebook.*