PETER RINDAL

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

PROFESSIONAL EXPERTISE

My expertise lies in the development and deployment of efficient methods for computing on encrypted data, i.e. secure multiparty computation protocols. Central to my success has been a holistic approach to the design, security analysis, and implementation of these protocols. Notable contributions are as follows.

Efficient methods for performing Private Set Intersection and encrypted database joins. In its simplest form, this technology allows two parties to identity common elements between sets held by each party without revealing any additional information. The protocols developed represent state of the art in a number of settings, e.g. semi-honest, malicious, honest majority, secret shared inputs, unbalanced sets. As a testament of the research, these protocols are currently deployed both within Visa and externally such as in the Microsoft Edge password manager.

Another area of focus has been the development of threshold cryptography. This line of research became a focus with the design of the DiSE protocol, the first highly efficient threshold scheme for authenticated encryption. This design has been further refined in the recent ParaDiSE protocol which offers more fine grained control and security guarantees. In addition, I have been the technical lead for implementing and deploying this technology at Visa for encryption, key management, and signing with threshold ECDSA.

Other areas of note include the design and implementation of efficient state of art methods for privacy preserving machine learning, i.e. regression, neural networks, decision trees. I lead the development of this technology at Visa with the goal to enable responsible data sharing with industry partners. Another Visa inspired application is privacy preserving biometric authentication where a client, e.g. card holder, wishes to authenticate to a server, e.g. Visa, using their biometrics without revealing the biometrics.

Finally, the development and security analysis of highly efficient low level cryptographic primitives, most notably Oblivious Transfer. In this area I have designed several of the state of art protocols (i.e. Endemic OT, Silent OT, Silver) and identified security vulnerabilities in existing constructions. In addition, I am the author of the industry leading open source library for performing efficient oblivious transfer.

EDUCATION

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

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

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

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 — January 2017 — June 2017
Security Research Consultant

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

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

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

PUBLICATIONS

Authors listed alphabetically

C1 – Shashank Agrawal, Wei Dai, Atul Luykx, Pratyay Mukherjee, Peter Rindal. *ParaDiSE: Efficient Threshold Authenticated Encryption in Fully Malicious Model.* Unpublished Manuscript 2022.

C2 – Srinivasan Raghuraman, Peter Rindal. *Blazing Fast PSI from Improved OKVS and Subfield VOLE.* In *IACR ePrint Archive 2022.*

C3 – Saikrishna Badrinarayanan, Eysa Lee, Peihan Miao, Peter Rindal. *Improved Multi-Party Fixed Point Multiplication.* Unpublished Manuscript 2022.

C4 – Saikrishna Badrinarayanan, Gayathri Garimella, Srinivasan Raghuraman, Peter Rindal. *Fast Fully Secret-Shared Private Multi-Set Intersection and SQL Joins with an Honest Majority.* Unpublished Manuscript 2022.

C5 – Saikrishna Badrinarayanan, Ranjit Kumaresan, Mihai Christodorescu, Vinjith Nagaraja, Karan Patel, Srinivasan Raghuraman, Peter Rindal, Wei Sun, Minghua Xu. *A Plug-n-Play Framework for Scaling Private Set Intersection to Billion-sized Sets.* In *IACR ePrint Archive 2022.*

C6 – Geoffroy Couteau, Srinivasan Raghuraman, Peter Rindal. *Silver: Silent VOLE and Oblivious Transfer from Hardness of Decoding Structured LDPC Codes.* In *CRYPTO: IACR International Cryptology Conference 2021.*

C7 – Peter Rindal, Phillipp Schoppmann. *VOLE-PSI: Fast OPRF and Circuit-PSI from Vector-OLE.* In *EUROCRYPT: IACR International Cryptology Conference 2021.*

C8 – 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.*

C9 – 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.*

C10 – 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.*

C11 – 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.*

C12 – Daniel Masny, Peter Rindal. *Endemic Oblivious Transfer.* In *CCS: ACM Conference on Computer and Communications Security 2019*

C13 – Adam Groce, Peter Rindal and Mike Rosulek. *Cheaper Private Set Intersection via Differentially Private Leakage.* In *PETS: Privacy Enhancing Technologies Symposium 2019.*

C14 – Daniel Demmler, Peter Rindal, Mike Rosulek and Ni Trieu. *PIR-PSI: Scaling Private Contact Discovery.* In *PETS: Privacy Enhancing Technologies Symposium 2018.*

C15 – Payman Mohassel and Peter Rindal. *ABY^3: A Mixed Protocol Framework for Machine Learning.* In *CCS: ACM Conference on Computer and Communications Security 2018.*

C16 – Shashank Agrawal, Payman Mohassel, Pratyay Mukherjee and Peter Rindal. *Threshold Authenticated Encryption.* In *CCS: ACM Conference on Computer and Communications Security 2018.*

C17 – 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.*

C18 – Peter Rindal and Roberto Trifiletti. *SplitCommit: Implementing and Analyzing Homomorphic UC Commitments.* In *IACR ePrint 2017.*

C19 – Melissa Chase, Ran Gilad-Bachrach, Kim Laine, Kristin Lauter and Peter Rindal. *Private Collaborative Neural Network Learning.* In *IACR ePrint 2017.*

C20 – Peter Rindal and Mike Rosulek. *Improved Private Set Intersection against Malicious Adversaries.* In *EUROCRYPT: IACR International Cryptology Conference 2017.*

C21 – Hao Chen, Kim Laine and Peter Rindal. *Fast Private Set Intersection from Homomorphic Encryption.* In *CCS: ACM Conference on Computer and Communications Security 2017.*

C22 – Peter Rindal and Mike Rosulek. *Malicious-Secure Private Set Intersection via Dual Execution.* In *CCS: ACM Conference on Computer and Communications Security 2017.*

C23 – 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.*

C24 – Ran Gilad-Bachrach, Kim Laine, Kristin Lauter, Peter Rindal and Mike Rosulek. *Secure Data Exchange: A Marketplace in the Cloud.* In *IACR ePrint 2016.*

C25 – Peter Rindal and Mike Rosulek. *Faster Malicious 2-party Secure Computation with Online/Offline Dual Execution.* In *USENIX Security Symposium 2016.*

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

S2 – Peter Rindal. *Hydra: Threshold ECDSA.* (Visa Internal)

S3 – Peter Rindal, et al.. *Visa Data Exchange: Secure Data Sharing Based on Private Set Intersection.* (Visa Internal)

S4 – Peter Rindal, Saikrishna Badrinarayanan. *PriTrees: Privacy Preserving Decision Tree Training and Inference.* (Visa Internal)

S5 – Peter Rindal. *Bio-Auth: Privacy Preserving Biometric Authentication for Visa-Checkout.* (Visa Internal)

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. *ABY^3: A Mixed Protocol Framework for Machine Learning.* (Open Source) `https://github.com/ladnir/aby3`

S8 – Peter Rindal. *Ivory-Runtime: A generic Secure Computation API for garbled circuits.* (Open Source) `https://github.com/ladnir/Ivory-Runtime`. Includes the protocols of:

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

S9 – 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].

S10 – Hao Chen, Kim Laine and Peter Rindal. *Asymmetric Private Set Intersection.* Deployed in Microsoft Edge. `https://www.microsoft.com/en-us/research/blog/password-monitor-safeguarding-passwords-in-microsoft-edge/`

S11 – Peter Rindal. *SMILY: Secure Multi-party Computation Library.* (Microsoft).

S12 – Peter Rindal and Roberto Trifiletti. *SplitCommit: A portable C++ implementation of the [FJNT16] XOR-homomorphic commitment scheme.* (Open Source) `https://github.com/AarhusCrypto/SplitCommit`

S13 – Peter Rindal. *Batch Dual Execution: Malicious secure online/offline MPC implementation.* (Open Source) `https://github.com/osu-crypto/batchDualEx`

SERVICE

E1 – External Reviewer, *CRYPTO: IACR International Cryptology Conference 2022.*

E2 – Committee Member, *EUROCRYPT: IACR International Cryptology Conference 2021.*

E3 – Committee Member, *CCS: ACM Conference on Computer and Communications Security 2020.*

E4 – External Reviewer, *EUROCRYPT: IACR International Cryptology Conference 2019.*

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

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

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

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

E9 – External Reviewer, *18th International Conference on Cryptology in India (Indocrypt 2017).* Chennai India on December 2017.

E10 – External Reviewer, *15th Theory of Cryptography Conference (TCC 2017).* Baltimore MD, USA on November, 2017.

E11 – External Reviewer, *2nd IEEE European Symposium on Security and Privacy (EuroS&P 2017).* Paris France on April 2017.

E12 – External Reviewer, *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, *Visa Research Manager. Now at Facebook.* payman.mohassel@gmail.com

R3 – Kim Laine, *Microsoft Research Mentor.* kim.laine@gmail.com