Yilei Chen

CONTACT

857-364-7472
chenyilei.ra@gmail.com
www.chenyilei.net

Visa Research
385 Sherman Ave.
Palo Alto, CA 94306

RESEARCH AREAS

Cryptography and cryptanalysis, theory of computation. Specific research interests include

- Lattice-based cryptography.
- Computing on encrypted data.
- Designing advanced encryption schemes, digital signatures, pseudorandom functions, hash functions, and program obfuscators.
- Developing algorithms and methodologies in cryptanalysis.

EMPLOYMENT

Visa Research, Palo Alto, CA, USA — June 2018 - Present

Staff research scientist in cryptography.
Research areas: post-quantum cryptography, computing on encrypted data.
Invited participant of "Lattices: Algorithms, Complexity, and Cryptography Program" at Simons Institute in Spring 2020.

SRI International, Menlo Park, CA, USA — June 2015 - August 2015

Research internship. Mentor: Dr. Mariana Raykova.
Research areas: program obfuscation, database delegation.

EDUCATION

Boston University, Boston, MA — January 2015 - May 2018

Doctor of Philosophy in Computer Science.
Dissertation: Hiding Secrets in Public Random Functions.
Thesis advisors: Professor Ran Canetti and Professor Leonid Reyzin.

Boston University, Boston, MA — September 2012 - January 2015

Master of Science in Computer Science.

Shanghai Jiao Tong University, Shanghai, China — September 2008 - June 2012

Bachelor of Science in Information Engineering. Member of the Honor Class.

PROGRAM COMMITTEE

- EUROCRYPT 2020 – 39th Annual Eurocrypt Conference
- ASIACRYPT 2019 – 25th Annual Asiacrypt Conference
- WAHC 2019 – 7th Workshop on Encrypted Computing & Applied Homomorphic Cryptography
- PKC 2018 – 21st International Conference on Practice and Theory of Public Key Cryptography

REVIEWER

- Annual Eurocrypt Conference (EUROCRYPT) 2019, 2018, 2017, 2016
- Annual International Cryptology Conference (CRYPTO) 2019, 2017
- Theory of Cryptography Conference (TCC) 2019, 2018, 2017, 2016-B, 2016-A
- IEEE Symposium on Foundations of Computer Science (FOCS) 2017
- Innovations in Theoretical Computer Science (ITCS) 2020
- ACM Conference on Computer and Communications Security (CCS) 2019, 2015
- IEEE Symposium on Security and Privacy (Oakland) 2019, 2018
- International Colloquium on Automata, Languages and Programming (ICALP) 2017
- The Cryptographer's Track of the RSA Conference (CT-RSA) 2020
- Journal of Information Security and Applications 2019
- Journal of Theoretical Computer Science 2019

ORGANIZATION COMMITTEE

- Fujitsu-Visa Post Quantum Crypto Day. — August 2019
- Boston University Security Seminar. — Fall 2017 & Spring 2018

Membership

- International Association for Cryptologic Research (IACR).

Research Internship Mentoring

- Fermi Ma (Princeton University) — Summer 2019 @Visa Research
- Sikhar Patranabis (IIT Kharagpur) — Summer 2019 @Visa Research
- Rouzbeh Behnia (University of South Florida) — Summer 2019 @Visa Research
- Nicholas Genise (University of California San Diego) — Summer 2018 @Visa Research
- Binyi Chen (University of California Santa Barbara) — Summer 2018 @Visa Research

Teaching Assistance

- Network Security (CS 558) — Fall 2015, Boston University
- Algebraic Algorithm (CS 235) — Fall 2014, Boston University
- Theory of Computing (CS 332) — Spring 2013, Boston University

Awards

- Research Excellence Award, Boston University — 2018
- Junyuan Scholarship, Tang Junyuan Educational Foundation — 2011, 2010, 2009, 2008
- Academic Excellence Scholarship, Shanghai Jiao Tong University — 2010, 2009

Publications

(In cryptography and theory of computation, authors are typically listed in alphabetical order.)

- *Hard Isogeny Problems over RSA Moduli and Groups with Infeasible Inversion.*
  Salim Ali Altuğ, Yilei Chen.
  25th Annual Asiacrypt Conference. ASIACRYPT 2019
- *Approximate Trapdoors for Lattices and Smaller Hash-and-Sign Signatures.*
  Yilei Chen, Nicholas Genise, Pratyay Mukherjee.
  25th Annual Asiacrypt Conference. ASIACRYPT 2019
- *Matrix PRFs: Constructions, Attacks, and Applications to Obfuscation.*
  Yilei Chen, Minki Hhan, Vinod Vaikuntanathan, Hoeteck Wee.
  17th IACR Theory of Cryptography Conference. TCC 2019
- *Continuous Space-Bounded Non-Malleable Codes from Stronger Proofs-of-Space.*
  Binyi Chen, Yilei Chen, Kristina Hostáková, Pratyay Mukherjee.
  39th Annual International Cryptology Conference. CRYPTO 2019
- *Fiat-Shamir: From Practice to Theory.*
  Ran Canetti, Yilei Chen, Justin Holmgren, Alex Lombardi, Guy N. Rothblum, Ron D. Rothblum, Daniel Wichs.
  51st Annual ACM Symposium on the Theory of Computing. STOC 2019
- *Traitor-Tracing from LWE Made Simple and Attribute-Based.*
  Yilei Chen, Vinod Vaikuntanathan, Brent Waters, Hoeteck Wee, Daniel Wichs.
  16th IACR Theory of Cryptography Conference. TCC 2018
- *GGH15 Beyond Permutation Branching Programs: Proofs, Attacks, and Candidates.*
  Yilei Chen, Vinod Vaikuntanathan, Hoeteck Wee.
  38th Annual International Cryptology Conference. CRYPTO 2018
- *Fiat-Shamir and Correlation Intractability from Strong KDM Encryption.*
  Ran Canetti, Yilei Chen, Leonid Reyzin, Ron D. Rothblum.
  37th Annual Eurocrypt Conference. EUROCRYPT 2018
- *Cryptanalyses of Candidate Branching Program Obfuscators.*
  Yilei Chen, Craig Gentry, Shai Halevi.
  36th Annual Eurocrypt Conference. EUROCRYPT 2017
- *Constraint-hiding Constrained PRFs for NC1 from LWE.*
  Ran Canetti, Yilei Chen.
  36th Annual Eurocrypt Conference. EUROCRYPT 2017
- *Adaptive Succinct Garbled RAM, or How to delegate your database.*
  Ran Canetti, Yilei Chen, Justin Holmgren, Mariana Raykova.
  14th IACR Theory of Cryptography Conference. TCC 2016-B
- *On the Correlation Intractability of Obfuscated Pseudorandom Functions.*
  Ran Canetti, Yilei Chen, Leonid Reyzin.
  13th IACR Theory of Cryptography Conference. TCC 2016-A

Invited Talks

- *Lattices, Multilinear Maps, and Program Obfuscation.*
  - Spring 2020 Lattices Program at Simons Institute — Berkeley, CA, USA, January 2020
  - Second Cryptography Innovation School — Shanghai, China, December 2019
  - Lattices and Crypto meeting at ENS Lyon — Lyon, France, July 2017

Seminar and Conference Talks

- *Hard Isogeny Problems over RSA Moduli and Groups with Infeasible Inversion.*
  - ASIACRYPT 2019 — Kobe, Japan, December 2019
  - KU Leuven COSIC seminar — Leuven, Belgium, November 2019
  - Shanghai University of Finance and Economics — Shanghai, China, November 2019
  - UC Berkeley crypto seminar — Berkeley, CA, USA, February 2019
  - Stanford security seminar — Stanford, CA, USA, December 2018
  - Shanghai Jiao Tong University seminar — Shanghai, China, November 2018
- *Approximate Trapdoors for Lattices and Smaller Hash-and-Sign Signatures.*
  - Second NIST PQC Standardization Conference — Santa Barbara, CA, USA, August 2019
- *Traitor-Tracing from LWE Made Simple and Attribute-Based.*
  - Theory of Cryptography Conference 2018 — Panaji, Goa, India, November 2018
- *GGH15 Beyond Permutation Branching Programs: Proofs, Attacks, and Candidates.*
  - CRYPTO 2018 — Santa Barbara, CA, USA, August 2018
- *Fiat-Shamir and Correlation Intractability from Strong KDM Encryption Schemes.*
  - EUROCRYPT 2018 — Tel Aviv, Israel, April 2018
  - MIT CIS seminar — Cambridge, MA, USA, December 2017
- *Cryptanalyses of Candidate Branching Program Obfuscators.*
  - EUROCRYPT 2017 — Paris, France, May 2017
  - Boston University security seminar — Boston, MA, USA, March 2017
- *Constraint-hiding Constrained PRFs for NC1 from LWE.*
  - Aarhus Cryptography Theory Seminar — Aarhus, Denmark, May 2017
  - EUROCRYPT 2017 — Paris, France, May 2017
  - Boston University cryptography seminar — Boston, MA, USA, April 2017
  - MIT CIS seminar — Cambridge, MA, USA, March 2017
- *Adaptive Succinct Garbled RAM, or How to delegate your database.*
  - Theory of Cryptography Conference 2016-B — Beijing, China, November 2016
  - DIMACS/MACS Workshop on Cryptography — Cambridge, MA, USA, June 2016
- *On the Correlation Intractability of Obfuscated Pseudorandom Functions.*
  - State Key Laboratory of Information Security — Beijing, China, October 2016
  - IST Austria — Klosterneuburg, Austria, March 2016
  - Theory of Cryptography Conference 2016-A — Tel Aviv, Israel, January 2016
  - MIT CIS seminar — Cambridge, MA, USA, December 2015
  - Boston University security seminar — Boston, MA, USA, October 2015

Patents

- *More Efficient Post-Quantum Signatures.*
  Yilei Chen, Nicholas Genise, Pratyay Mukherjee. — Patent application filed
- *Continuous Space Bounded Non-Malleable Codes.*
  Binyi Chen, Yilei Chen, Pratyay Mukherjee. — Patent application filed