Chang Liu

CONTACT INFORMATION

Department of EECS
University of California, Berkeley
Address: 2728 Carlson Blvd
Richmond, CA, USA, 94804
Homepage: https://people.eecs.berkeley.edu/ liuchang/

Mobile: 240-472-8855
liuchang@eecs.berkeley.edu

RESEARCH INTERESTS

Security, Programming Language, Deep Learning

EDUCATION

University of Maryland, College Park, MD, USA

PhD, Computer Science Sept. 2012 to Aug. 2016

Shanghai Jiao Tong University, Shanghai, China

Master, Computer Science, Sept. 2009 to March 2012

Bachelor, Computer Science, Sept. 2005 to July 2009

WORKING EXPERIENCE

University of California, Berkeley, *Postdoc*	**Aug. 2016 to now**
University of California, Berkeley, *Visiting Student*	**Oct. 2015 to Aug. 2016**
Google, New York, *Intern*	**May 2015 to Aug. 2015**
Microsoft Research, Redmond, *Intern*	**June 2013 to Aug. 2013**
University of Maryland, *Research Assistant*	**Jan. 2013 to Aug. 2015**
University of Maryland, *Teaching Assistant*	**Sept. 2012 to Jan. 2013**
Microsoft Research Asia, *Intern*	**Sept. 2011 to July 2012**
IBM China Research Lab, *Intern*	**July 2008 to Nov. 2008**

AWARDS

Academic Awards

- Best Paper Award, AISec 2017
- First Place of Best Paper Award in Applied Cyber Security Research, CSAW 15
- John Vlissides Award, 2015
- Best Paper Award, ASPLOS 2015
- HLI Award for Secure Multiparty Computation in the iDash Secure Genomics Analysis Competition, 2015
- SoCC '14 Student Scholarship
- Programming Language Mentoring Workshop Schoarship Award, 2015
- 2013 The NSA Best Scientific Cybersecurity Paper Award.
- IEEE Symposium on Security and Privacy 2014 Student Travel Grants
- NSF Travel Grants (ACM SIGSPATIAL GIS 2013)
- USENIX OSDI '12 Student Grant
- AAAI-12 Scholarship
- Semantic Web Science Association Student Travel Award, ISWC 2010, ISWC 2011
- Best Paper Award, CSWS 2010

University

- Future Faculty Fellow, 2015
- Finalist of Facebook Fellowship, 2015
- Outstanding Early Graduate Student Award, University Fellowship, 2014
- Finalist of Symantec Graduate Fellowship, 2014
- Dean Fellowship, University of Maryland, 2012, 2013
- Bo Shi Scholarship, 2011
- Shanghai Jiao Tong University Scholarship Class A, 2006, 2007, 2008, 2010
- Shanghai Jiao Tong University Scholarship Class B, 2009

- Du Shuwu Scholarship, 2008
- Microsoft Young Fellowship, 2008
- Irving T. Ho Fellowship, 2005

ACM International Collegiate Programming Contest

- ACM/ICPC World Final, 5th Place, Silver Medal, Asia Champion, April 2006
- ACM/ICPC World Final, 8th Place, Silver Medal, March 2007
- ACM/ICPC Asia Regional Contest Champion, 2005(Taipei), 2005(Tokyo), 2006((Tokyo)
- ACM/ICPC Asia Regional Contest, Second Place, 2005(Tokyo), 2006(Kaohsiung)

Referenced Journal Papers

[1] **Chang Liu**, Guilin Qi, Haofen Wang, Yong Yu, *Reasoning with Large Scale Ontologies in Fuzzy pD* using MapReduce*, In **IEEE Computational Intelligence Magazine** (Impact Factor 2.833) Volume 7, Issue 2, May 2012, Pages 54-66

[2] Haofen Wang, Thanh Tran, **Chang Liu**, Linyun Fu, *Lightweight Integration of IR & DB for Scalable Hybrid Search with Integrated Ranking Support*, In **the Journal of Web Semantics** (Impact Factor 2.789) Volume 9, Issue 4, December 2011, Pages 490-503

[3] **Chang Liu**, Haofen Wang, Yong Yu, Linhao Xu, *Towards Efficient SPARQL Query Processing on RDF Data*, **Tsinghua Science & Technology**, Volume 15, Issue 6, Pages 613-622 (**CSWS '10 Best Paper Award**)

Referenced Conference Papers

[1] Xiaojun Xu, Xinyun Chen, **Chang Liu**, Anna Rohrbach, Trevor Darell, and Dawn Song, *Fooling Vision and Language Models Despite Localization and Attention Mechanism*, to appear in Proceedings of the Thirtieth IEEE/CVF Conference on Computer Vision and Pattern Recognition (**CVPR '18**), Salt Lake City, Utah, USA

[2] Huichen Li, Xiaojun Xu, **Chang Liu**, Teng Ren, Kun Wu, Xuezhi Cao, Weinan Zhang, Yong Yu, Dawn Song, *A Machine Learning Approach To Prevent Malicious Calls Over Telephony Networks*, to appear in Proceedings of the 39th IEEE Symposium on Security and Privacy (**Oakland '18**), San Francisco, CA, USA

[3] Xinyun Chen, **Chang Liu**, and Dawn Song, *Tree-to-tree Neural Networks for Program Translation*, to appear in Proceedings of 6th International Conference on Learning Representations Workshop (**ICLR Workshop '18**), Vancouver, CANADA

[4] Xinyun Chen, **Chang Liu**, and Dawn Song, *Towards Synthesizing Complex Programs From Input-Output Examples*, to appear in Proceedings of 6th International Conference on Learning Representations (**ICLR '18**), Vancouver, CANADA

[5] **Chang Liu**, Bo Li, Yevgeniy Vorobeychik, and Alina Oprea, *Robust Linear Regression Against Training Data Poisoning*, in Proceedings of 10th ACM Workshop on Artificial Intelligence and Security (**AISec 17)**, Dallas, TX, USA
(**Best Paper Award**)

[6] Xiaojun Xu, **Chang Liu**, Qian Feng, Heng Yin, Dawn Song, and Le Song, *Neural Network-based Graph Embedding for Cross-Platform Binary Code Similarity Detection*, in Proceedings of 24th ACM Conference on Computer and Communications Security (**CCS '17**), Dallas, TX, USA

[7] Yanpei Liu, Xinyun Chen, **Chang Liu**, and Dawn Song, *Delving into Transferable Adversarial Examples and Black-box Attacks*, in Proceedings of International Conference on Learning Representation 2017 (**ICLR '17**), France

[8] Xinyun Chen, **Chang Liu**, Richard Shin, Dawn Song, and Mingcheng Chen, *Latent Attention For If-Then Program Synthesis*, in Proceedings of the 29th Advances in Neural Information Processing Systems (**NIPS '16**), 2016, Barcelona, SPAIN

[9] Xiaojing Liao, **Chang Liu**, Damon McCoy, Elaine Shi, and Raheem Beyah, *Characterizing Long-tail SEO Spam on Cloud Web Hosting Services*, in Proceedings of the 25th International World Wide Web Conference (**WWW '16**), 2016, Montreal, Canada

[10] Dana Dachman-Sole, **Chang Liu**, Charalampos Papamanthou, Elaine Shi, and Uzi Vishkin, *Oblivious Network RAM and Leveraging Parallelism to Achieve Obliviousness*, in Proceedings of the 21st Annual International Conference on the Theory and Application of Cryptology and Information Security (**Asiacrypt '15**)

[11] **Chang Liu**, *Trace Oblivious Computation*, in Proceedings of SPLASH Companion 2015, Pittsburgh, PA, USA (Doctoral Symposium)
(John Vlissides Award, 2015)

[12] **Chang Liu**, Xiao Shaun Wang, Kartik Nayak, Yan Huang, and Elaine Shi, *ObliVM: A Generic, Customizable, and Reusable Secure Computation Architecture*, in Proceedings of IEEE Symposium on Security and Privacy 2015 (**Oakland '15**)
(**First Place of Best Paper Award in Applied Cyber Security Research, CSAW 15**)

[13] **Chang Liu**, Michael Hicks, Austin D. Harris, Mohit Tiwari, Martin Maas, and Elaine Shi, *GhostRider: A Hardware-Software System for Memory Trace Oblivious Computation*, in Proceedings of 20th International Conference on Architectural Support for Programming Languages and Operating Systems (**ASPLOS '15**), Istanbul, TURKEY
(**Best Paper Award**)

[14] **Chang Liu**, Jiaxing Zhang, Hucheng Zhou, Sean McDirmid, Zhenyu Guo, and Thomas Moscibroda, *Automating Distributed Partial Aggregation*, in Proceedings of 2014 ACM Symposium on Cloud Computing (**SoCC '14**), Seattle, WA, USA

[15] Xiao Shaun Wang, Kartik Nayak, **Chang Liu**, T-H. Hubert Chan, Elaine Shi, Emil Stefanov, and Yan Huang, *Oblivious Data Structures*, in Proceedings of 21st ACM Conference on Computer and Communications Security (**CCS '14**), Scottsdale, Arizona, USA

[16] **Chang Liu**, Yan Huang, Elaine Shi, Jonathan Katz, and Michael Hicks, *Automating Efficient RAM-Model Secure Computation*, in Proceedings of the IEEE Symposium on Security and Privacy 2014 (**Oakland '14**), San Jose, CA, USA.

[17] **Chang Liu**, Jacopo Urbani, Guilin Qi, *Efficient RDF Stream Reasoning with GPU*, in Proceedings of International World Wide Web Conference 2014 (**WWW '14**), Seoul, Korea (Poster)

[18] **Chang Liu**, Brendan C. Fruin, Hanan Samet, *SAC: Semantic Adaptive Caching for Spatial Mobile Applications*, in Proceedings of 21st ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems (**SIGGIS '13**), Orlando, FLorida, USA

[19] **Chang Liu**, Michael Hicks, Elaine Shi, *Memory Trace Oblivious Program Execution*, In Proceedings of 2013 IEEE 26th Computer Security Foundations Symposium (**CSF '13**), New Orlean, Louisiana, USA
(**2013 the NSA Best Scientific Cybersecurity Paper Award.**)

[20] Zhenyu Guo, Xuepeng Fan, Rishan Chen, Jiaxing Zhang, Hucheng Zhou, Sean McDirmid, **Chang Liu**, Wei Lin, Jingren Zhou, Lidong Zhou, *Spotting Code Optimizations in Data-Parallel Pipelines through PeriSCOPE*, In Proceedings of 10th USENIX Symposium on Operating System Design and Implementation (**OSDI '12**), Pages 121-134, Hollywood, California, USA

[21] Zhangquan Zhou, Guilin Qi, **Chang Liu**, Pascal Hitzler, Raghava Mutharaju, *Reasoning with Fuzzy-EL+ Ontologies Using MapReduce*, In Proceedings of the 20th European Conference on Artificial Intelligence (**ECAI '12**), Pages 933-934, 2012, Montpellier, France (Short paper)

[22] **Chang Liu**, Guilin Qi, *Toward Scalable Reasoning over Annotated RDF Data Using MapReduce*, In Proceedings of the 6th International Conference on Web Reasoning and Rule Systems (**RR '12**), Pages 238-241, 2012, Vienna, Austria
(Technical Communications)

[23] **Chang Liu**, Guilin Qi, Yong Yu, *Large Scale Temporal RDFS Reasoning Using MapReduce*, In Proceedings of the Twenty-Sixth AAAI Conference (**AAAI '12**), Pages 2441-2442, 2012, Toronto, Canada (Student Poster)

[24] **Chang Liu**, Guilin Qi, Haofen Wang, Yong Yu, *Large Scale Fuzzy pD* Reasoning using MapReduce*, In Proceedings of the 10th International Semantic Web Conference (**ISWC '11**), Pages 405-420, 2011, Bonn, Germany

[25] **Chang Liu**, Guilin Qi, Haofen Wang, Yong Yu, *Fuzzy Reasoning over RDF Data Using OWL Vocabulary*, In Proceedings of the 2011 IEEE/WIC/ACM International Conference on Web Intelligence (**WI '11**), Pages 162-169, 2011, Lyon, France

[26] Haofen Wang, Thanh Tran, **Chang Liu**, *CE2: towards a large scale hybrid search engine with integrated ranking support*, In Proceedings of the 20th ACM Conference on Information and Knowledge Management (**CIKM '08**), Pages 1323-1324, 2008, Napa Valley, California, USA (Poster)

Technical Reports

- Nicholas Carlini, **Chang Liu**, Jernej Kos, Úlfar Erlingsson, and Dawn Song, *The Secret Sharer: Measuring Unintended Neural Network Memorization & Extracting Secrets*, arXiv preprint arXiv:1802.08232

- Qiuyuan Huang, Li Deng, Dapeng Wu, **Chang Liu**, and Xiaodong He, *Attentive Tensor Product Learning for Language Generation and Grammar Parsing*,
arXiv preprint arXiv:1802.07089

- Xinyun Chen, **Chang Liu**, Bo Li, Kimberly Lu, and Dawn Song, *Targeted Backdoor Attacks on Deep Learning Systems Using Data Poisoning*, arXiv preprint arXiv:1712.05526, Dec, 2017
Media coverage: Motherboard

- David Darais, **Chang Liu**, Ian Sweet, and Michael Hicks, *A Language for Probabilistically Oblivious Computation*, arXiv preprint arXiv:1711.09305, Nov, 2017

- Xiaojun Xu, **Chang Liu**, and Dawn Song, *SQLNet: Generating Structured Queries From Natural Language Without Reinforcement Learning*, arXiv preprint arXiv:1711.04436, Nov, 2017

- Xiaojun Xu, Xinyun Chen, **Chang Liu**, Anna Rohrbach, Trevor Darell, and Dawn Song, *Can you fool AI with adversarial examples on a visual Turing test?*, arXiv preprint arXiv:1709.08693, Sep, 2017

- Xinyun Chen, **Chang Liu**, and Dawn Song, *Learning Neural Programs To Parse Programs*, arXiv preprint arXiv:1706.01284, June, 2017

- **Chang Liu**, Bo Li, Yevgeniy Vorobeychik, and Alina Opera, *Robust High-Dimensional Linear Regression*, arXiv preprint arXiv:1608.02257, Aug, 2016.

- **Chang Liu**, Michael Hicks, Austin D. Harris, Mohit Tiwari, Martin Maas, and Elaine Shi, *GhostRider: A Hardware-Software System for Memory Trace Oblivious Computation*, Technical Report CS-TR-5041, University of Maryland, Department of Computer Science, Jan. 2015.

- Xiao Shaun Wang, **Chang Liu**, Kartik Nayak, Yan Huang, and Elaine Shi, *iDASH Secure Genome Analysis Competition using ObliVM*, in ePrint, URL https://eprint.iacr.org/2015/191.pdf
(**HLI Award for Secure Multiparty Computation in the iDash Secure Genomics Analysis Competition, 2015**)

- **Chang Liu**, Jiaxing Zhang, Hucheng Zhou, Sean McDirmid, Zhenyu Guo, and Thomas Moscibroda, *Automating Distributed Partial Aggregation*, In Technical Report. URL http://www.cs.umd.edu/ liuchang/paper/pa-socc2014-tr.pdf.

- **Chang Liu**, Yan Huang, Elaine Shi, Jonathan Katz, and Michael Hicks, *Automating Efficient RAM-Model Secure Computation*, Technical Report, University of Maryland, Department of Computer Science, 2014

- **Chang Liu**, Michael Hicks, Elaine Shi, *Memory Trace Oblivious Program Execution*, Technical Report CS-TR-5020, University of Maryland Department of Computer Science, 2013.

GRANT

- Enhancing Security Using Deep Learning Techniques. Center for Long-Term Cybersecurity, Berkeley, $100,000, 2018

TALKS

- Opening Remark, at Deep Learning and Security Workshop Research Forum 2017, Singapore Dec 14, 2017

- Robust Linear Regression Against Training Data Poisoning, at AISec 2017, Nov 3, 2017

- Neural Network-based Graph Embedding for Cross-Platform Binary Code Similarity Detection, at CCS 2017, Oct 30, 2017

- Synergy Between Deep Learning and Security, Google Cloud AI, Sep 28, 2017

- Synergy Among Deep Learning, Security, and Programming Languages, MSR, Jun 29, 2017

- Toward building Secure applications using Programming Language and Deep Learning, Google Brain, Jun 2, 2017

- Adversarial Deep Learning, at Deep Learning Security Workshop, Singapore, Feb 19, 2017

- Exploring New Attack Space on Adversarial Deep Learning at GeekPwn, Palo Alto, Oct 23, 2016

- Oblivious Network RAM and Leveraging Parallelism to Achieve Obliviousness, at ASIACRYPT, Dec 2, 2015

- ObliVM: A Programming Framework for Secure Computation at Oakland, at CSAW 2015, Nov 13, 2015

- Trace Oblivious Program Execution: A Programming Language Approach in Security, at SPLASH Doctoral Symposium, Oct 27, 2015

- ObliVM + Obliv-C week presenter, Sep, 22-25, at Cornell

- ObliVM: A Programming Framework for Secure Computation at Oakland 2015, May 19, 2015

- ObliVM: A Programming Framework for Secure Computation at DCAPS 2015, May 4, 2015
- Memory Trace Oblivious Program Execution for Cloud Computing at HotSoS 2015 (Invited talk), April 21, 2015
- GhostRider: A Hardware-Software System for Memory Trace Oblivious Computation at ASPLOS 2015, March 16, 2015
- Automating Distributed Partial Aggregation at SoCC 2014, Nov 3, 2014
- Memory Trace Oblivious Program Execution at DCAPS, May 23, 2014
- Automating Efficient RAM-Model Secure Computation at Oakland 2014, May 21, 2014
- SAC: Semantic Adaptive Caching for Spatial Mobile Applications at SIGGIS 2013, Nov 7, 2013
- Memory Trace Oblivious Program Execution at LOLA 2013, June 29, 2013
- Memory Trace Oblivious Program Execution at CSF 2013, June 26, 2013
- Large Scale Fuzzy pD* Reasoning using MapReduce at ISWC 2011, Oct 25, 2011
- Fuzzy Reasoning over RDF Data Using OWL Vocabulary at WI 2011, Aug 24, 2011

Services

Program Committee

- ICML 2018, GameSec 2018 (Program Committee)
- NDSS 2018 (Program Committee, Travel Grant Committee)
- Machine Learning and Computer Security Workshop 2017, co-located with NIPS 2017 (Program Chair)
- 2nd Singapore CyberSecurity Consortium (SGCSC) Research Forum, Dec 2017 (Program Chair)
- 1st Singapore CyberSecurity Consortium (SGCSC), Feb 2017 (General Chair)
- Oakland 2016 (Student PC)

Reviewer

- Oakland 2018, NDSS 2018, NIPS 2016, CCS 2016, Oakland 2016, POPL 2016, CSF 2014, 2015, ESWC 2011, 2014, SUM 2012
- TKDE 2013, The Journal of Web Semantics 2011

Advising Students

- Xinyun Chen (now a PhD student at UC Berkeley)
- Yanpei Liu
- Haobin Ni (now a PhD student at Cornell)
- Xiaojun Xu (now an undergraduate student at Shanghai Jiao Tong University)

Referees

Prof. Dawn Song
Professor
University of California, Berkeley
dawnsong@cs.berkeley.edu

Prof. Trevor Darrell
Professor
University of California, Berkeley
Email: trevordarrell@berkeley.edu

Prof. Elaine Shi
Associate Professor
Cornell University
runting@gmail.com

Prof. Michael Hicks
Professor
University of Maryland, College Park
mwh@cs.umd.com