

Vladimir Kolesnikov
Professor and Senior Associate Chair
School of Cybersecurity and Privacy
and
Professor
School of Computer Science

College of Computing
Georgia Institute of Technology
kolesnikov@gatech.edu

Contents

I. Earned Degrees	2
II. Employment History	2
III. Honors and Awards	2
IV. Research, Scholarship, and Creative Activities	2
IV.A. Published Books, Book Chapters, and Edited Volumes	3
IV.A.1. Books	3
IV.A.2. Refereed Books Chapters	3
IV.A.3. Edited Volumes	3
IV.B. Refereed Publications and Submitted Articles	4
IV.B.1. Published and Accepted Journal Articles	4
IV.B.2. Conference Presentation with Proceedings (Refereed)	5
IV.B.3. Other refereed material	10
IV.B.4. Submitted Journal Articles (with date of submission)	10
IV.C. Other Publications and Creative Products	10
IV.D. Presentations	11
IV.F Other Scholarly and Creative Accomplishments	13
IV.G Societal and Policy Impacts	13
IV.H Other Professional Activities	13
V. Education	14
V.A. Courses Taught	14
V.B. Individual Student Guidance	14
V.B.1. Ph.D. Students	14
V.B.2. M.Sc. Students	15
V.B.3. Undergraduate Students	15
V.B.4. Service on thesis or dissertation committees	15
V.B.5. Mentorship of postdoctoral fellows or visiting scholars	16
V.C. Educational Innovations and Other Contributions	17
VI. Service	18
VI.A. Professional Contributions	18
VI.B. Public and Community Service	19
VI.C. Institute Contributions	19

I. Earned Degrees

Degree	Year	University	Field
Ph.D.	2006	University of Toronto, Toronto, Canada Ph.D. Advisors: Ian F. Blake and Charles Rackoff	Computer Science
M.Sc.	1996	Rochester Institute of Technology, Rochester, NY M.Sc. Advisor: Stanislaw Radziszowski	Computer Science
B.Sc.	1995	Rochester Institute of Technology, Rochester, NY	Mathematics

II. Employment History

Title	Organization	Years
Professor	College of Computing Georgia Institute of Technology	08/2021 – present
Associate Professor	College of Computing Georgia Institute of Technology	01/2018–08/2021
Member of Technical Staff	Bell Labs, Murray Hill, NJ	07/2006–12/2017
Researcher	Bioscrypt Inc., Toronto, ON, Canada	08/2004-03/2005
Researcher	Kasten Chase, Toronto, ON, Canada	04/2001-10/2001
Software Engineer	Algorithmics Inc., Toronto ON, Canada	10/1999-09/2000
Software Engineer	The MathWorks Inc., Natick, MA	05/1997-09/1999

III. Honors and Awards

- *Computing Dean's Award: The James D. Lester Endowment Award*. Georgia Tech, 2020.
Established by Faye R. and James D. Lester III, this annual award will be presented to a faculty member who has made significant, high quality, innovative contributions, to their field of study, visibly impacting on or more mission areas. It is expected that such contributions would have brought widespread recognition to the researcher, his/her lab, and the Institute. This award is specifically directed to research in internet phenomena (this can include but is not limited to animation, gaming, email, music, video, television and film).
- *Medal for Service to the Faculty of Mathematics*, Grodno State University, Belarus, 2006.
This is the award of the department in recognition of the service of providing a series of lectures over multiple years. Lecture topics include cryptography and general-audience talks on US/Canadian education system.

IV. Research, Scholarship, and Creative Activities

Asterisk indicates those that resulted from work done at Georgia Tech. Names of student co-authors are in boldface.

NOTE: Author order usually follows the convention of the venue. E.g., security papers are usually: students in order of contribution followed by faculty in order of contribution. In crypto venues, the author order in the papers is *alphabetic*.

IV.A. Published Books, Book Chapters, and Edited Volumes

IV.A.1. Books

1. * David Evans, Vladimir Kolesnikov and Mike Rosulek. A Pragmatic Introduction to Secure Multi-Party Computation. Foundations and Trends in Privacy and Security: Vol. 2: No. 2-3, pp 70-246. <http://dx.doi.org/10.1561/33000000019>
Book webpage is <http://securecomputation.org/>. Chinese translation is available <https://item.jd.com/13302742.html>.

IV.A.2. Refereed Books Chapters

1. **K. Järvinen**, V. Kolesnikov, A.-R. Sadeghi, and **T. Schneider**, Efficient secure two-party computation with untrusted hardware tokens. In Towards Hardware Intrinsic Security: Foundation and Practice (A.-R. Sadeghi, ed.), Information Security & Cryptography, Springer, Heidelberg, Germany, 2010.

IV.A.3. Edited Volumes

1. * Jing Deng, Vladimir Kolesnikov, Alexander A. Schwarzmann. Cryptology and Network Security - 22nd International Conference, CANS 2023, Augusta, GA, USA, October 31 - November 2, 2023, Proceedings. Lecture Notes in Computer Science 14342, Springer 2023, ISBN 978-981-99-7562-4
2. * Alexandra Boldyreva and Vladimir Kolesnikov. 26th IACR International Conference on Practice and Theory of Public-Key Cryptography, Atlanta, GA, USA, May 8-10, 2023, Proceedings, Revised Selected Papers. Lecture Notes in Computer Science 13940 and 13941.
3. * Clemente Galdi and Vladimir Kolesnikov. Journal of Computer Security (Elsevier), Special issue on selected papers from SCN 2020. 30(1): 1-2 (2022)
4. * Selected papers from CSCML 2020, the 4th International Symposium on Cyber Security Cryptology and Machine Learning. Inf. Comput. 285(Part): 104927 (2022)
5. * Clemente Galdi and Vladimir Kolesnikov Security and Cryptography for Networks 12th International Conference, SCN 2020, Amalfi, Italy, September 14-16, 2020, Proceedings. Springer Lecture Notes in Computer Science, issue 12238
6. * Shlomi Dolev, Vladimir Kolesnikov, Sachin Lodha, Gera Weiss. Cyber Security Cryptography and Machine Learning Fourth International Symposium, CSCML 2020, Beer-Sheva, Israel, July2-3, 2020, Proceedings. Springer Lecture Notes in Computer Science, issue 12161.

7. Tal Malkin, Vladimir Kolesnikov, Allison Bishop Lewko, Michalis Polychronakis. Applied Cryptography and Network Security - 13th International Conference, ACNS 2015, New York, NY, USA, June 2-5, 2015, Revised Selected Papers. Lecture Notes in Computer Science 9092, Springer 2015, ISBN 978-3-319-28165-0



IV.B. Refereed Publications and Submitted Articles

IV.B.1. Published and Accepted Journal Articles

1. * Shlomi Dolev, Juan A. Garay, Niv Gilboa, Vladimir Kolesnikov, Muni Venkateswarlu Kumaraman-galam: Perennial secure multi-party computation of universal Turing machine. In *Theor. Comput. Sci.* 769: 43-62 (2019)
2. Y. Kim, V. Kolesnikov and M. Thottan. Resilient End-to-End Message Protection for Cyber-Physical System Communications, in *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2478-2487, July 2018. doi: 10.1109/TSG.2016.2613545
3. Juan A. Garay, Vladimir Kolesnikov, Rae McLellan. MAC Precomputation with Applications to Secure Memory. In *ACM Transactions on Privacy and Security (TOPS)*, 2016.
4. Shlomi Dolev, Juan A. Garay, Niv Gilboa, Vladimir Kolesnikov, **Yelena Yuditsky**. Towards efficient private distributed computation on unbounded input streams. In *J. Mathematical Cryptology* 9(2): 79-94 (2015).
5. Vladimir Kolesnikov, Ahmad-Reza Sadeghi, and Thomas Schneider. A systematic approach to practically efficient general two-party secure function evaluation protocols and their modular design. In *Journal of Computer Security (JCS)*, 21(2): 283-315 (2013).
6. Vladimir Kolesnikov, Abdullatif Shikfa, On the limits of Privacy Provided by Order-Preserving Encryption. In *Bell Labs Technical Journal (BLTJ)* 17(3): 135-146 (2012).
7. Vladimir Kolesnikov, Wonsuck Lee, MAC Aggregation Resilient to DoS Attacks. In *International Journal of Security and Networks (IJSN)* 7(2): 122-132 (2012).
8. Vijay Gurbani and Vladimir Kolesnikov. A Survey and Analysis of Media Keying Techniques in the Session Initiation Protocol (SIP). In *IEEE Communications Surveys and Tutorials* 13(2): 183-198 (2011)
9. Georg Hampel and Vladimir Kolesnikov. Securing Host-based Mobility and Multi-homing Protocols Against on-path Attackers. In *Journal of Communications (JCM) Special Issue on Seamless Mobility in Wireless Networks*, JCM 6(1): 101-114 (2011)
10. Young-Jin Kim, Marina Thottan, Vladimir Kolesnikov, Wonsuck Lee, Decentralized and Data-centric Information Infrastructure for Next-Generation Smart Grid. In *IEEE Communications Magazine* 48(11): 58-65 (2010)
11. Vladimir Kolesnikov, Advances and Impact of Secure Function Evaluation, In *Bell Labs Technical Journal (BLTJ)*, 14(3): 187-192 (2009)

12. Ian F. Blake and Vladimir Kolesnikov, One-round secure comparison of integers. In *Journal of Mathematical Cryptography*, 3(1): 37-68 (2009).

IV.B.2. Conference Presentation with Proceedings (Refereed)

1. * **James Choncholas**, Ketan Bhardwaj, Vladimir Kolesnikov, Ada Gavrilovska. Angler: Dark Pool Resource Allocation. In ACM/IEEE Symposium on Edge Computing (SEC) 2023.
2. * **Yibin Yang**, David Heath, Carmit Hazay, Vladimir Kolesnikov, Muthuramakrishnan Venkatasubramanian: Batchman and Robin: Batched and Non-batched Branching for Interactive ZK. CCS 2023: 1452-1466. **Distinguished paper award.** 
3. * **Yibin Yang, Stanislav Peceny**, David Heath, Vladimir Kolesnikov: Towards Generic MPC Compilers via Variable Instruction Set Architectures (VISAs). CCS 2023: 2516-2530
4. * David Heath, Vladimir Kolesnikov, Rafail Ostrovsky: Tri-State Circuits - A Circuit Model that Captures RAM. CRYPTO (4) 2023: 128-160
5. Vladimir Kolesnikov, **Stanislav Peceny**, Ni Trieu, Xiao Wang: Fast ORAM with Server-Aided Pre-processing and Pragmatic Privacy-Efficiency Trade-Off. CSCML 2023: 439-457
6. * **Anasuya Acharya**, Carmit Hazay, Vladimir Kolesnikov, Manoj Prabhakaran: SCALES - MPC with Small Clients and Larger Ephemeral Servers. TCC (2) 2022: 502-531
7. * **Abida Haque, David Heath**, Vladimir Kolesnikov, Steve Lu, Rafail Ostrovsky, **Akash Shah**. Garbled Circuits With Sublinear Evaluator. Eurocrypt 2022.
8. * **David Heath**, Vladimir Kolesnikov, Rafail Ostrovsky. EpiGRAM: Practical Garbled RAM. Eurocrypt 2022. **Best paper award.** 
9. * **Yibin Yang, David Heath**, Vladimir Kolesnikov, David Devecsery. EZEE: Epoch Parallel Zero Knowledge for ANSI C. In EuroS&P 2022.
10. * Christopher Cordi, Michael P. Frank, Kasimir Gabert, Carollan Helinski, Ryan C. Kao, Vladimir Kolesnikov, **Abraham Ladha** and Nicholas Pattengale. Auditable, Available and Resilient Private Computation on the Blockchain via MPC. In CSCML 2022.
11. * **David Heath**, Vladimir Kolesnikov. PrORAM: Fast $O(\log n)$ Authenticated Shares ZK ORAM. Asiacrypt 2021.
12. * **David Heath**, Vladimir Kolesnikov, **Stanislav Peceny**. Garbling, stacked and staggered: Faster k -out-of- n garbled function evaluation. Asiacrypt 2021.
13. * **David Heath**, Vladimir Kolesnikov: One Hot Garbling. CCS 2021
14. * **David Heath, Yibin Yang**, David Devecsery, and Vladimir Kolesnikov. Zero knowledge for everything and everyone: Fast ZK processor with cached ORAM for ANSI C programs. In 2021 IEEE Symposium on Security and Privacy (SP), 2021.

15. * **Erkam Uzun**, Simon Pak Ho Chung, Vladimir Kolesnikov, Alexandra Boldyreva, Wenke Lee. Fuzzy Labeled Private Set Intersection with Applications to Private Real-Time Biometric Search. In USENIX Security 2021.
16. * **Erkam Uzun, Carter Yagemann**, Simon P. Chung, Vladimir Kolesnikov, Wenke Lee: Cryptographic Key Derivation from Biometric Inferences for Remote Authentication. AsiaCCS 2021
17. * **David Heath**, Vladimir Kolesnikov, **Jiahui Lu**: Efficient Generic Arithmetic for KKW - Practical Linear MPC-in-the-Head NIZK on Commodity Hardware Without Trusted Setup. CSCML 2021
18. * **David Heath**, Vladimir Kolesnikov, LogStack: Stacked Garbling with $O(b \log b)$ Computation. EUROCRYPT 2021
19. * **David Heath**, Vladimir Kolesnikov, **Stanislav Peceny**, Amortizing Multiplication Triples Across Conditionals. Public Key Cryptography 2021
20. * **David Heath** and Vladimir Kolesnikov, A 2.1 KHz Zero-Knowledge Processor with BubbleRAM. In CCS 2020.
21. * **David Heath**, Vladimir Kolesnikov, **Stanislav Peceny**, MOTIF: (Almost) Free Branching in GMW via Vector-Scalar Multiplication. In Asiacrypt 2020.
22. * **David Heath** and Vladimir Kolesnikov. Stacked Garbling: Garbled Circuit Proportional to Longest Execution Path. In Crypto 2020.
23. * **David Heath**, Vladimir Kolesnikov. Stacked Garbling for Disjunctive Zero-Knowledge Proofs. In Eurocrypt 2020.
24. * Vladimir Kolesnikov, Mike Rosulek, **Ni Trieu, Xiao Wang**. Scalable Private Set Union from Symmetric-Key Techniques. In Asiacrypt 2019.
25. * Cheng Hong, Jonathan Katz, Vladimir Kolesnikov, Wen-jie Lu, **Xiao Wang**. Covert Security with Public Verifiability: Faster, Leaner, and Simpler. EUROCRYPT (3) 2019: 97-121.
26. * Ketan Bhardwaj, Ada Gavrilovska, Vlad Kolesnikov, **Matt Saunders, Hobin Yoon, Mugdha Bondre, Meghana Babu**, Jacob Walsh. Addressing the Fragmentation Problem in Distributed and Decentralized Edge Computing: A Vision. IEEE International Conference on Cloud Engineering (IC2E) 2019: 156-167
27. * Vladimir Kolesnikov. Free IF : How to Omit Inactive Branches and Implement S-Universal Garbled Circuit (Almost) for Free. *ASIACRYPT (3)* pp. 34-58, 2018.
28. * Jonathan Katz, Vladimir Kolesnikov, **Xiao Wang**. Improved Non-Interactive Zero Knowledge with Applications to Post-Quantum Signatures. *ACM Conference on Computer and Communications Security (CCS)* pp. 525-537, 2018.
29. * Vladimir Kolesnikov, Mike Rosulek, **Ni Trieu**. SWiM: Secure Wildcard Pattern Matching From OT Extension. In *Financial Cryptography and Data Security*, 2018.
30. Sean Kennedy, Vladimir Kolesnikov, Gordon Wilfong: Overlaying Conditional Circuit Clauses for Secure Computation. In *Asiacrypt*, 2017.

31. Vladimir Kolesnikov, Jesper Buus Nielsen, Mike Rosulek, **Ni Trieu**, **Roberto Trifiletti**. DUPLO: Unifying Cut-and-Choose for Garbled Circuits. In *24th ACM Conference on Computer and Communications Security (CCS)*, 2017.
32. Vladimir Kolesnikov, **Naor Matania**, Benny Pinkas, Mike Rosulek, **Ni Trieu**. DUPLO: Practical Multi-party Private Set Intersection from Symmetric-Key Techniques. In *24th ACM Conference on Computer and Communications Security (CCS)*, 2017.
33. **Xiong Fan**, **Chaya Ganesh**, Vladimir Kolesnikov. Hashing Garbled Circuits for Free. In *Eurocrypt*, 2017.
34. Vladimir Kolesnikov, Hugo Krawczyk, Yehuda Lindell, **Alex J. Malozemoff**, Tal Rabin. Attribute-based Key Exchange with General Policies. In *23rd ACM Conference on Computer and Communications Security (CCS)*, 2016.
35. Vladimir Kolesnikov, Ranjit Kumaresan, Mike Rosulek, **Ni Trieu**. Efficient Batched Oblivious PRF with Applications to Private Set Intersection. In *23rd ACM Conference on Computer and Communications Security (CCS)*, 2016.
36. Vladimir Kolesnikov, **Alex J. Malozemoff**. Public Verifiability in the Covert Model (Almost) for Free. In *ASIACRYPT (2) 2015*: 210-235, 2015.
37. Vladimir Kolesnikov, Ranjit Kumaresan. On Cut-and-Choose Oblivious Transfer and Its Variants. In *ASIACRYPT (1) 2015*: 386-412, 2015.
38. **Ben A. Fisch**, **Binh Vo**, **Fernando Krell**, **Abishek Kumarasubramanian**, Vladimir Kolesnikov, Tal Malkin, Steven M. Bellovin. Malicious-Client Security in Blind Seer: A Scalable Private DBMS. In *IEEE Symposium on Security and Privacy 2015*: 395-410, 2015
39. Thomas Fossati, Vijay K. Gurbani, Vladimir Kolesnikov. Love All, Trust Few: on Trusting Intermediaries in HTTP. In *HotMiddlebox@SIGCOMM 2015*: 1-6, 2015.
40. Vladimir Kolesnikov, Payman Mohassel, Ben Riva, Mike Rosulek. Richer Efficiency/Security Trade-offs in 2PC. In *TCC (1) 2015*: 229-259, 2015.
41. Vladimir Kolesnikov, Payman Mohassel, Mike Rosulek. FleXOR: Flexible Garbling for XOR Gates That Beats Free-XOR. *CRYPTO (2) 2014*: 440-457, 2014.
42. **Yan Huang**, Jonathan Katz, Vladimir Kolesnikov, **Ranjit Kumaresan**, **Alex J. Malozemoff**. Amortizing Garbled Circuits. In *CRYPTO (2) 2014*: 458-475, 2014.
43. Ran Canetti, Vladimir Kolesnikov, Charles Rackoff, Yevgeniy Vahlis. Secure Key Exchange and Sessions without Credentials. In *SCN 2014*: 40-56, 2014.
44. Paul Giura, Vladimir Kolesnikov, **Aris Tentes**, Yevgeniy Vahlis. Efficient Network-Based Enforcement of Data Access Rights. In *SCN 2014*: 236-254, 2014.
45. **Vasilis Pappas**, **Fernando Krell**, **Binh Vo**, Vladimir Kolesnikov, Tal Malkin, Seung Geol Choi, **Wesley George**, Angelos D. Keromytis, Steve Bellovin. Blind Seer: A Scalable Private DBMS. In *IEEE Symposium on Security and Privacy 2014*: 359-374, 2014.

46. Vladimir Kolesnikov and **Ranjit Kumaresan**, Improved OT Extension for Transferring Short Secrets. In *33rd International Cryptology Conference CRYPTO 2013*, 2013.
47. Shlomi Dolev, Juan Garay, Niv Gilboa, Vladimir Kolesnikov and **Yelena Yuditsky**. Towards Efficient Private Distributed Computation on Unbounded Input Streams. In *11th International Conference on Applied Cryptography and Network Security (ACNS)*, 2013.
48. Young Jin Kim, Vladimir Kolesnikov, Marina Thottan. TSAF: Tamper-resistant and Scalable Mutual Authentication Framework for Plug-in EV Charging. In *IEEE SmartGridComm 2013*.
49. Young Jin Kim, Vladimir Kolesnikov, Marina Thottan. Resilient End-to-End Message Protection for Large-scale Cyber-Physical System Communications. In *IEEE SmartGridComm 2012*.
50. Vladimir Kolesnikov, **Ranjit Kumaresan**, and Abdullatif Shikfa. Efficient Verification of Input Consistency in Server-Assisted Secure Function Evaluation. In *Computer and Network Security (CANS) 2012*.
51. Shlomi Dolev, Juan Garay, Niv Gilboa, Vladimir Kolesnikov, **Yelena Yuditsky**. Brief Announcement: Efficient Distributed Private Computation on Unbounded Input Streams. In *The 26th International Symposium on Distributed Computing (DISC) 2012*.
52. Dov Gordon, Jonathan Katz, Vladimir Kolesnikov, **Fernando Krell**, Tal Malkin, **Mariana Raykova**, Yevgeniy Vahlis. Secure Two-Party Computation in Sublinear (Amortized) Time. In *19th ACM Conference on Computer and Communications Security (CCS) 2012*.
53. Vladimir Kolesnikov, MAC Aggregation with Message Multiplicity. In *8th Conference on Security and Cryptography for Networks (SCN), 2012*.
54. Vladimir Kolesnikov and **Ranjit Kumaresan**, Improved Secure Two-Party Computation via Information-Theoretic Garbled Circuits. In *8th Conference on Security and Cryptography for Networks (SCN), 2012*.
55. Shlomi Dolev, Juan Garay, Niv Gilboa, Vladimir Kolesnikov, Secret Sharing Krohn-Rhodes: Private and Perennial Distributed Computation. In *Second Symposium on Innovations in Computer Science (ICS) 2011*.
56. Young-Jin Kim, Vladimir Kolesnikov, Hongseok Kim, and Marina Thottan, SSTP: a Scalable and Secure Transport Protocol for Smart Grid Data Collection. In *IEEE SmartGridComm 2011*.
57. Vladimir Kolesnikov, Wonsuck Lee, and Junhee Hong, MAC Aggregation Resilient to DoS Attacks. In *IEEE SmartGridComm 2011*.
58. Shlomi Dolev, Juan Garay, Niv Gilboa, Vladimir Kolesnikov, Brief Announcement: Swarming Secrets. In *Twenty-Ninth Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing (PODC) 2010*.
59. Vladimir Kolesnikov. A Security Enhancement and Proof for Authentication and Key Agreement (AKA). In *7th Conference on Security and Cryptography for Networks (SCN) 2010*.

60. **Kimmo Järvinen**, Vladimir Kolesnikov, Ahmad-Reza Sadeghi, and **Thomas Schneider**. Garbled Circuits for Leakage-Resilience: Hardware Implementation and Evaluation of One-Time Programs. In *Workshop on Cryptographic Hardware and Embedded Systems 2010 (CHES 2010)*.
61. Vladimir Kolesnikov. Truly Efficient String Oblivious Transfer Using Resettable Tamper-Proof Tokens. In *Theory of Cryptography Conference (TCC)*, 2010.
62. **Kimmo Järvinen**, Vladimir Kolesnikov, Ahmad-Reza Sadeghi, **Thomas Schneider**. Embedded SFE: Offloading Server and Network using Hardware Tokens. In *14th International Conference on Financial Cryptography and Data Security (FC 2010)*, 2010.
63. Ken Budka, Jayant Deshpande, John Hobby, Young-Jin Kim, Vladimir Kolesnikov, Wonsuck Lee, Marina Thottan, Thomas Reddington, Chris A. White, Jung-In Choi, Junhee Hong, Jinho Kim, Wonsuk Ko, Young-Woo Nam, Sung- Yong Sohn. GERI Bell Labs Smart Grid Research Focus: Economic Modeling, Networking, and Security and Privacy. In *IEEE SmartGridComm*, 2010.
64. Georg Hampel and Vladimir Kolesnikov. Lightweight Security Solution for Host-Based Mobility & Multi-Homing Protocols. In *IEEE Globecom 2010 Workshop on Seamless Wireless Mobility (SWiM)*, 2010.
65. Vijay Gurbani and Vladimir Kolesnikov. Work in Progress: A secure and lightweight scheme for media keying in the Session Initiation Protocol (SIP). In *IPTComm 2010: Principles, Systems and Applications of IP Telecommunications*, 2010.
66. Mauro Barni, **Pierluigi Failla**, Vladimir Kolesnikov, **Riccardo Lazzeretti**, **Annika Paus**, Ahmad-Reza Sadeghi, and **Thomas Schneider**. Efficient privacy-preserving classification of ECG signals. In *1st IEEE International Workshop on Information Forensics and Security (IEEE WIFS)*, 2009.
67. Shlomi Dolev, Juan Garay, Niv Gilboa and Vladimir Kolesnikov, Swarming Secrets. In *47th Annual Allerton Conference*, 2009.
68. Vladimir Kolesnikov, Ahmad-Reza Sadeghi and **Thomas Schneider**, Improved Garbled Circuit Building Blocks and Applications to Auctions and Computing Minima. In *Computer and Network Security (CANS) 2009*.
69. Mauro Barni, **Pierluigi Failla**, Vladimir Kolesnikov, **Riccardo Lazzeretti**, Ahmad-Reza Sadeghi and **Thomas Schneider**, Secure Evaluation of Private Linear Branching Programs with Medical Applications. In *European Symposium on Research in Computer Security (ESORICS) 2009*.
70. Juan Garay, Vladimir Kolesnikov and Rae McLellan, MAC Precomputation with Applications to Secure Memory, In *Information Security Conference (ISC) 2009*.
71. Vladimir Kolesnikov and **Thomas Schneider**, Improved Garbled Circuit: Free XOR Gates and Applications. In *International Colloquium on Automata, Languages and Programming (ICALP) 2008*.
72. Vladimir Kolesnikov and Charles Rackoff, Password Mistyping in Two-Factor-Authenticated Key Exchange. In *International Colloquium on Automata, Languages and Programming (ICALP) 2008*.
73. Vladimir Kolesnikov and **Thomas Schneider**, A Practical Universal Circuit Construction and Secure Evaluation of Private Functions. In *Financial Cryptography and Data Security Conference (FC) 2008*.

74. Ian F. Blake and Vladimir Kolesnikov, Conditional Encrypted Mapping and Comparing Encrypted Numbers. In *Financial Cryptography and Data Security Conference (FC) 2006*.
75. Vladimir Kolesnikov and Charles Rackoff, Key Exchange Using Passwords and Long Keys. In *Theory of Cryptography Conference 2006*. Springer-Verlag LNCS Vol. 3876.
76. Vladimir Kolesnikov, Gate Evaluation Secret Sharing and Secure One-Round Two-Party Computation. In *Advances of Cryptology – ASIACRYPT 2005*. Springer-Verlag LNCS Vol. 3788.
77. Ian F. Blake and Vladimir Kolesnikov, Strong Conditional Oblivious Transfer and Computing on Intervals. In *Advances of Cryptology – ASIACRYPT 2004*. Springer-Verlag LNCS Vol. 3329.

IV.B.3. Other refereed material

No data.

IV.B.4. Submitted Journal Articles (with date of submission)

No data.

IV.C. Other Publications and Creative Products

Manuscripts in preparation or submission:

NIST standardization submission for Post-Quantum Secure Digital Signature Algorithms

Title: *Picnic: A Family of Post-Quantum Secure Digital Signature Algorithms*.

Status: *Picnic advanced to third round as alternate candidate (July 22, 2020)*

The Picnic family of digital signature algorithms is designed to provide security against attacks by quantum computers, in addition to attacks by classical computers. The building blocks are a zero-knowledge proof system (with post-quantum security), and symmetric key primitives like hash functions and block ciphers, with well-understood post-quantum security. Picnic does not require number-theoretic, or structured hardness assumptions (lattices, codes, isogenies, etc.).

Core algorithm is based on the MPC-in-the-head line of work. Joint work with Jonathan Katz, and Xiao Wang “Improved Non-Interactive Zero Knowledge with Applications to Post-Quantum Signatures” is the most recent improvement to the submitted algorithm.

Picnic was designed by a group of cryptographers from Aarhus University, AIT Austrian Institute of Technology GmbH, DFINITY, Graz University of Technology, Georgia Tech, Microsoft Research, Northwestern University, Princeton University, Technical University of Denmark and the University of Maryland.

The team includes Melissa Chase, David Derler, Steven Goldfeder, Jonathan Katz, Vladimir Kolesnikov, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig, Xiao Wang, and Greg Zaverucha.

Submission in full detail, including reference implementation is available at <https://microsoft.github.io/Picnic/>.

* In July 2020, Picnic advanced to third round as alternate candidate. Alternate candidates follow a 1-year delayed timeline to standardization to allow for more analysis and maturity. Some alternate candidates were selected in part because of their potential. See <https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions> and <https://csrc.nist.gov/News/2020/pqc-third-round-candidate-announcement>.

Technical Reports:

1. Vladimir Kolesnikov, Ganapathy Sundaram, IBAKE: Identity-Based Authenticated Key Exchange Protocol. *IACR Cryptology ePrint Archive 2011: 612 (2011)*.
2. A number of reports in support of WiMAX effort in Sprint Nextel and in Alcatel-Lucent Wireless Business Unit, 2007
3. Biometric Key Binding. Technical report to Canadian National Research Council's Industrial Research Assistance Program (NRC-IRAP). With Omid Jahromi, Rene McIver, Colin Soutar and Alex Stoianov, 2005
4. Binding Strong Keys to Fingerprints Securely and Privately. Technical Report, Bioscrypt, Inc., 2005
5. Efficient Storage Security. Technical Report, Kasten Chase, Inc., 2001
6. Efficient Broadcast Encryption. Technical Report, Kasten Chase, Inc., 2001

IV.D. Presentations

Summer School: Invited Lecturer

1. 2020 Summer School on MPC in Copenhagen. May 18-22, 2020. School is co-funded by IACR (International Association for Cryptologic Research), organized by a leading MPC research group, and taught by leading MPC researchers. <https://events.au.dk/mpcsummerschool2020/>. Update: School postponed due to the virus.

Invited Speaker (Travel expences at least partially paid by the host/organizers)

1. Speaker and Panelist. Plenary Panel: Grand Challenges in Cyber Security and Privacy. IEEE TPS / CIC / CogMI 2023, November 1-3, 2023. Atlanta, GA, USA
2. Keynote. Brown University, ICERM. MAPPS Workshop on Privacy and Ethics in Pandemic Data Collection and Processing. Efficient and scalable multiparty computation. January 2023.
3. New Directions in Garbled Circuits. Milan Theory Workshop. <https://www.unibocconi.eu/wps/wcm/connect/ev/events/bocconi+events/milano+theory+workshop>,
4. SysML4Health: Scalable Systems for ML-driven Analytics in Healthcare. 2021. Invited speaker. <https://mlsys.org/virtual/2021/workshop/1641> March 2021
5. Private DB – Big-size searching from (many) small-size MPC instances. In *ICERM/Brown University workshop on Encrypted Search*. Jun 10 - 14, 2019

6. Covert Security with Public Verifiability: Faster, Leaner, and Simpler. In DIMACS/MACS Workshop on Usable, Efficient, and Formally Verified Secure Computation. Invited speaker. Mar 13-14, 2019.
7. Faster Secure Computation from Overlaying Garbled Circuit Clauses. In *Security and Privacy Day, Stony Brook University National Security Institute*. Invited speaker. Oct 13, 2017.
8. *Theory and Practice of Multi-Party Computation Workshop*, Bristol, UK. April 3-7, 2017. Invited speaker.
9. Practical Private DB Querying. In *IEEE 4th Annual Symposium on Cybersecurity and Internet of Things (IoT)*, FDU, Sep 28, 2016. Featured speaker and panelist.
10. Invited participant and panelist. In *NSF workshop on Data Science for Secure and Privacy-aware (DSSP) Large Data Management and Mining*. September 26-27, 2016.
11. Overlaying Branches in Garbled Circuits. In *Workshop on Theory and Practice of Secure Multiparty Computation*, Aarhus, May 30-June 3, 2016. Invited speaker.
12. Practical Private DB Querying. In *Simons Institute workshop on Securing Computation*, June 8-12, 2015. Invited speaker.
13. Practical Private Database Querying. In *Workshop on Theory and Practice of Secure Multiparty Computation*, Aarhus, May 5-9, 2014. Invited speaker.
14. MAC Precomputation with Applications to Secure Memory. In *Warsaw Workshop on Leakage, Tampering and Viruses*, University of Warsaw, June 2-7, 2013. Invited speaker.
15. Scalable Private Database Querying for Arbitrary Formulas. In *DIMACS Workshop on Current Trends in Cryptology*, NYC, April 29 - May 1, 2013. Invited speaker.
16. Practical Private Database Querying. In *Applied Multi-Party Computation Workshop*, MSR Redmond, February 20-21, 2013. Invited speaker and panelist.

Other Workshop presentations

1. Private DB – Big-size searching from (many) small-size MPC instances. In *ODSA: Oblivious Data Structures and Algorithms*. Bertinoro, Italy, Jul 14-17, 2019
2. Covert Security with Public Verifiability: Faster, Leaner, and Simpler. In *Theory and Practice of Multi-Party Computation Workshop*, Bar-Ilan University, Tel-Aviv, Israel, June 17-20, 2019.
3. Proving anything quickly and privately with secure computation *IISP Cybersecurity Lecture Series, Georgia Tech*, Aug 2018.
4. Secure Key Exchange and Sessions without Credentials. In *Secure Key Exchange and Channel Protocols (SKECH III)*, Bertinoro, Italy, July 2018.
5. SWiM: Secure Wildcard Pattern Matching From OT Extension. Presentation at
 - *Theory and Practice of Multi-Party Computation Workshop*, Aarhus, May 2018.
 - *Encryption for Secure Search and other Algorithms 2 (ESSA2)*, Bertinoro, Italy, July 2018.

6. Enabling data sharing with secure computation. In *DIMACS/Northeast Big Data Hub Workshop on Privacy and Security for Big Data*, Rutgers University, April 24-25, 2017.
7. Overlaying Branches in Garbled Circuits. In *DIMACS Workshop on Cryptography and its Interactions*, Rutgers University, July 11 - 13, 2016.
8. Attribute-based Key Exchange for General Policies. In *Secure Key Exchange and Channel Protocols (SKECH II)*, Bertinoro, Italy, July 3-6, 2016.
9. Shlomi Dolev, Juan Garay, Niv Gilboa, Vladimir Kolesnikov, Private and Perennial Distributed Computation. In *Workshop on Cryptography and Security in Clouds*, Zurich, March 15-16, 2011.
10. Dov Gordon, Jonathan Katz, Vladimir Kolesnikov, Tal Malkin, Mariana Raykova, Yevgeniy Vahlis, Amortized Sublinear Secure Multi Party Computation. In *Workshop on Cryptography and Security in Clouds*, Zurich, March 15-16, 2011.
11. Mauro Barni, Pierluigi Failla, Vladimir Kolesnikov, Riccardo Lazzeretti, Ahmad-Reza Sadeghi, and Thomas Schneider, Combining Signal Processing and Cryptographic Protocol Design for Efficient ECG Classification. In *The International Workshop on Signal Processing in the Encrypted Domain (SPEED 2009)*.
12. Vladimir Kolesnikov, Ahmad-Reza Sadeghi and Thomas Schneider, How to Combine Homomorphic Encryption and Garbled Circuits: Improved Circuits and Computing the Minimum Distance Efficiently. In *The International Workshop on Signal Processing in the Encrypted Domain (SPEED 2009)*.
13. Juan Garay, Vladimir Kolesnikov and Rae McLellan, Efficient Techniques for Securing Off-Chip Memory. In *Computer & Electronics Security Applications Rendez-vous (C&ESAR)*, 2008.

IV.F Other Scholarly and Creative Accomplishments

59 patents granted, 9 patents pending (as of 2017). All patents related to cryptography, security and networking.

IV.G Societal and Policy Impacts

No Data.

IV.H Other Professional Activities

- Visited Ivan Visconti at Univeristy of Salerno for 1-week collaboration visit. July 2019.

- Visited Carmit Hazay and Benny Pinkas at Bar-Ilan University for 2-week collaboration visit. June 2019.
- Visited Jonathan Katz at UMD for 1-week collaboration visit. June 2019.
- DIMACS visitor. Collaboration visit sponsored by DIMACS. Boston University. March 13-19, 2019.
- Visited Jonathan Katz at UMD (salary and travel paid by Jonathan) for 1-month collaboration visit. July 2018.

V. Education

V.A. Courses Taught

<u>Semester/Year</u>	<u>Course</u>	<u>Number of Students</u>	<u>Comments</u>
Fall 2018	CS 8803 Secure Multiparty Computation	8 + 3 audit	CIOS 5.0
Spring 2019	CS 4803/8803 Blockchain and Cryptocurrency	40 + several audit	
Fall 2019	CS 8803 Secure Multiparty Computation	8 + several audit	CIOS 5.0
Spring 2020	CS 4803/8803 Blockchain and Cryptocurrency	44	
Fall 2020	CS 8803 Secure Multiparty Computation	14	
Spring 2021	CS 4803/8803 Blockchain and Cryptocurrency	42 (completed) + several audit	CIOS 4.9
Fall 2021	CS 8803 Secure Multiparty Computation	about 20	
Spring 2022	CS 4803/8803 Blockchain and Cryptocurrency	100 cap	
Spring 2023	CS 4803/8803 Blockchain and Cryptocurrency	100 cap	

V.B. Individual Student Guidance

V.B.1. Ph.D. Students

- *David Heath*. PhD 2022. ZK proofs and secure computation. First job - Assistant Prof at UIUC.
- *Yibin Yang*. ZK proofs and secure computation. 2019-
- *Jiahui Lu*. Co-advised with Sasha Boldyreva. Secure computation. PhD → MS completed.
- *Stan Pečený*. ZK Proofs and secure computation. 2019-
- *Lucien Ng*. Secure computation. 2022-

V.B.2. M.Sc. Students

- *Patrick Friedrich* (Georgia Tech). Exploring blockchain applications. 2018-2019
- *Abraham Ladha* (Georgia Tech). MPC for blockchain. 2019-2021

V.B.3. Undergraduate Students

- *Jack Wolfard* (Georgia Tech). Zero-knowledge compiler for ANSI C. 2020-2021
- *Abraham Ladha* (Georgia Tech). Working on improving prior private database work. 2018-2019

V.B.4. Service on thesis or dissertation committees

1. *Tianxin Tang* (Georgia Tech). Defended in 2021.
2. *Erkam Uzun* (Georgia Tech). Defended in 2021.
3. *Zhengxian He* (Georgia Tech).
4. *Shan Chen* (Georgia Tech). Defended Jan 2020.
5. *Xiao Wang* (UMD). Defended June 2018. Xiao is now Assistant Professor at Northwestern University.
6. *Ni Trieu* (Oregon State U). Ni defended in March 2020. She accepted Assistant Professor position at Arizona State Univeristy.
7. *Chaya Ganesh* (NYU), defended 2017. Chaya is Assistant Professor at the Computer Science department at IISc, Bangalore.
8. *Luis Brandao* (CMU), defended 2016. Luis is now at NIST.
9. *Alex Malozemoff* (UMD), defended 2016. Alex is now a researcher at Galois.
10. *Wilko Henecka* (University of Adelaide, Australia), defended 2015. Wilko is now a researcher at CSIRO's Data61, Australian research organization.
11. *Fernando Krell* (Columbia University), defended 2015. Fernando is now a researcher at Dreamlab Technologies and instructor at Universidad Catolica de Chile.
12. *Virendra Kumar* (Georgia Tech), defended 2012. Virendra is now Director of OEM Consulting at OnBoard Security, Inc.

V.B.5. Mentorship of postdoctoral fellows or visiting scholars

As a Member of Technical Staff at Bell Labs, I sponsored (paid with my grants) and mentored 18 Ph.D. students. My mentees are now in positions such as Full Professor, Assistant Professor, NIST, industry and government research, etc.

1. *Xiao Wang* (UMD). Summer intern 2017. Work on garbled circuits and attribute-based authentication, ONR. Xiao is now Assistant Professor at Northwestern University.
2. *Ni Trieu* (Oregon State U). Summer intern 2017. Work on private DB. Ni joined Arizona State University as Assistant Professor.
3. *Ni Trieu* (Oregon State U). Summer intern 2016. Work on garbled circuits and private set intersection, ONR.
4. *Leo Fan* (Cornell). Summer intern 2016. Work on garbled circuits, ONR.
5. *Chaya Ganesh* (NYU). Summer intern 2016. Work on garbled circuits and credentials, ONR. Chaya is Assistant Professor at Computer Science department at IISc, Bangalore.
6. *Luke Kowalczyk* (Columbia U). Summer intern 2015. Work on attribute-based authentication, ONR. Luke is now at a financial startup.
7. *Luis Brandao* (CMU). Summer intern 2015. Work on secure computation, ONR. Luis is now at NIST.
8. *Alex Malozemoff* (UMD). Intern 2015. Work on secure computation and attribute-based authentication, ONR. Alex is now a researcher at Galois.
9. *Abhishek Kumarasubramanian* (UCLA). Summer intern 2013. Work on the IARPA project. Abhishek is now a security engineer at Google.
10. *Aris Tentes* (NYU). Summer intern 2012. Work on DB policy enforcement. Aris is now a Quant and Strategist, working in investment management.
11. *Fernando Krell* (Columbia U). Summer intern 2012. Work on the IARPA project. Fernando is now a researcher and engineer at Dreamlab Technologies.
12. *Vasilis Pappas* (Columbia U). Summer intern 2012. Work on the IARPA project. Vasilis (independently) won the \$200K Microsoft Blue Hat prize for his security work. Vasilis is now a Senior Research Scientist at Appthority.
13. *Ranjit Kumaresan* (UMD). Summer Intern 2011. Work on efficiency improvements of SFE. Ranjit is now at Visa Research.
14. *Sriram Nandha Premnath* (Utah). Summer Intern 2011. Work on Smart Grid security. Sriram is now at Qualcomm Research.
15. *Virendra Kumar* (GATech). Summer Intern 2010. Worked on secure computation. Virendra is now Director of OEM Consulting at OnBoard Security, Inc.
16. *Gilles Baechler* (EPFL, Switzerland). Intern 2010. Worked on malicious-secure two-party computation. Gilles is now Ph.D. student at EPFL.
17. *Bhavana Kanukurthi* (Boston U). Intern 2009. Worked on key exchange protocols. Bhavana is now Assistant professor in Indian Institute of science, Bangalore.

18. *Thomas Schneider* (Bochum, Germany). Intern 2007 (6 months). Co-supervised his diploma thesis, a finalist in German computer science thesis competition (*Informatiktage*). Thomas is now Full Professor in TU Darmstadt.

V.C. Educational Innovations and Other Contributions

Book being adopted for crypto courses.

My recent book is being used in teaching crypto and privacy courses (in addition to courses taught by book authors at Georgia Tech, UVa and Oregon State):

- Berkeley, BU. Fall 2019: Law for Algorithms. <http://www.bu.edu/riscs/courses/>.
BU: CS 791 / JD 673
UC Berkeley: CS 294
- Stanford. Spring 2019, Spring 2020 CS 355: Topics in Cryptography. <https://crypto.stanford.edu/cs355/19sp/schedule/>, <https://crypto.stanford.edu/cs355/20sp/schedule/>
- Brown. Fall '19: Brown CS 2950-v: Topics in Applied Cryptography: Crypto for Social Good <http://cs.brown.edu/~seny/2950v/>.
- GWU. Spring 2020, CSIC 3907-83/6907-81 - Advanced Cryptography. https://www2.seas.gwu.edu/~arkady/teaching/advanced_crypto/s20/
- and more..

The book is: David Evans, Vladimir Kolesnikov and Mike Rosulek. A Pragmatic Introduction to Secure Multi-Party Computation. Foundations and Trends in Privacy and Security: Vol. 2: No. 2-3, pp 70-246. <http://dx.doi.org/10.1561/33000000019>, Book webpage is <http://securecomputation.org/>

Course Development

CS 8803 Secure Multiparty Computation

Developed from scratch this graduate course, introducing students *without assuming prior cryptography background* to classic and state-of-the-art techniques in the area. Material is covered in-depth, and requires students to design protocols and write formal reduction-style proofs of security. A proof usually includes exhibiting a simulator of players' view in the ideal model, and proving indistinguishability of the simulator output from the players' view in the real execution.

Topics covered include basic primitives (encryption, oblivious transfer, commitment, etc.) and advanced constructions, such as state-of-the-art garbled circuit (GC), Goldreich-Micali-Wigderson protocol, information-theoretic GC, zero-knowledge proofs. In addition to standard semi-honest and malicious models, we considered alternative security models, such as covert and publicly-verifiable covert.

Students report that it was the heaviest but very enjoyable course they took.

CIOS 5.0 in 2018 and 2019.

CS 4803/8803 Blockchain and cryptocurrency

Developed from scratch (based on the quite informal Princeton blockchain book) this cross-listed graduate course, taking a formal cryptographic approach to blockchain *without assuming prior cryptography*

background. Material is covered with respect to formal definitions of standard crypto primitives. E.g. we introduce IND-CPA secure encryption schemes and homeworks include proofs with respect to the challenge games described in the definitions. At the same time, we have a lot of breadth in the blockchain space, covering Bitcoin and other simple currencies, as well as classic crypto e-cash schemes (e.g. by Chaum). We also have programming projects and a term paper reporting on blockchain literature.

CIOS 4.6-4.8 in 2019 and 4.9 in 2021.

VI. Service

VI.A. Professional Contributions

1. Program co-chair (with Jing Deng) of CANS 2023
2. Program co-chair (with Sasha Boldyreva) of PKC 2023
3. Member of the Board of Directors of IACR (International Association for Cryptologic Research) for 2020 and 2021
4. General Chair of CRYPTO 2021
5. Program Chair of the 12th Security and Cryptography for Networks Conference (SCN 2020)
6. Program Chair of 4th International Symposium on Cyber Security Cryptology and Machine Learning (CSCML 2020)
7. General Chair of ACNS 2015
8. Program Committee Member of
 - (a) Crypto'24
 - (b) Crypto'22
 - (c) CSCML'22
 - (d) CSCML'21
 - (e) RSA 2020,
 - (f) Crypto 2019,
 - (g) Security and Privacy (Oakland) 2019, 2020,
 - (h) International Symposium on Cyber Security Cryptography and Machine Learning (CSCML) 2017,
 - (i) Eurocrypt 2017,
 - (j) ACM CCS 2016,
 - (k) IEEE SwSTE 2016,
 - (l) ACNS 2016,
 - (m) CT-RSA 2015,
 - (n) IH & MMSEC 2014,

- (o) PKC 2014,
 - (p) Workshop on Applied Homomorphic Cryptography 2013, 2014, 2015, 2016, 2017,
 - (q) LATINCRYPT 2012,
 - (r) IEEE SmartGridComm 2012, 2014,
 - (s) CANS 2010,
 - (t) Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS) 2010,
 - (u) CANS 2009,
 - (v) INSCRYPT 2007.
9. Reviewer for top conferences and journals (all IACR venues, Nature, etc.)
 10. Reviewer of several NSF and ISF proposals.

Standards Work

1. *WiMAX security and authentication*. One of three or four WiMAX Forum's PKI security experts. Editor of WiMAX "Server Certificate Profile" and "Device Certificate Profile" standards documents. Actively participated in WiMAX Forum's effort in standardizing use of certificates in authentication devices and subscribers. Lead meetings, edited standards documents. Responsible for technical aspects of WiMAX authentication solutions of Alcatel-Lucent and Sprint Nextel. Represented Alcatel-Lucent and Sprint Nextel in standards meetings. Wrote a number of technical reports influencing and supporting standards decisions. June 2007-2010.

VI.B. Public and Community Service

1. Math Kangaroo Center Director (Emory University). K-12 students, 2022-
2. Math Club in Clairemont Elementary School, Decatur, GA (2020)

VI.C. Institute Contributions

1. SCP Senior Associate Chair (March 2022-)
2. GT College of Computing Reappointment, Promotion, and Tenure (RPT) Committee Chair (2022-)
3. SCP Reappointment, Promotion, and Tenure (RPT) Committee Chair (2021-2022)
4. SCS and SCP Faculty Recruiting Committee (2020-2021)
5. SCS Faculty Recruiting Committee (2019-2020)
6. Area coordinator for Security (2018-2022)
7. MSc Admissions coordinator for Cyber Security (2018-2019)