SOPHIA YAKOUBOV

PERSONAL INFORMATION

email sophia.yakoubov@gmail.com

website http://web.mit.edu/sonka89/www/

EDUCATION

2019-Present Aarhus University

Currently working as a post-doctoral researcher at Aarhus University.

2017–2020 Boston University

Graduated with Ph.D. degree in Computer Science. GPA: 4.0/4.0

2014–2016 Boston University

Graduated with Master of Science degree in Computer Science. GPA: 4.0/4.0

2007–2011 Massachusetts Institute of Technology

Graduated with Bachelor of Science degree in Mathematics with Computer Science. GPA: 4.4/5.0

PUBLISHED TECHNICAL PAPERS

Broadcast Secret-Sharing, Bounds and Applications

I. Damgård, K. G. Larsen, **S. Yakoubov** (ITC 2021)

Turning HATE Into LOVE: Compact Homomorphic Ad Hoc Threshold Encryption for Scalable MPC

L. Reyzin, A. Smith, **S. Yakoubov** (CSCML 2021)

The Rise of Paillier: Homomorphic Secret Sharing and Public-Key Silent OT

C. Orlandi, P. Scholl, **S. Yakoubov** (Eurocrypt 2021)

Stronger Security and Constructions of Multi-Designated Verifier Signatures

I. Damgård, H. Haagh, R. Mercer, A. Nitulescu, C. Orlandi, **S. Yakoubov** (TCC 2020)

Universally Composable Accumulators

R. Canetti, F. Baldimtsi, **S. Yakoubov** (CT-RSA 2020)

Fuzzy Password-Authenticated Key Exchange

P.A. Dupont, J. Hesse, D. Pointcheval, L. Reyzin, **S. Yakoubov** (Eurocrypt 2018)
This work was also presented at TPMPC 2018.

Catching MPC Cheaters: Identification and Openability

R. Cunningham, B. Fuller, **S. Yakoubov** (ICITS 2017)
This work was also presented at TPMPC 2017.

Efficient Accumulators with Applications to Anonymity-Preserving Revocation

F. Baldimtsi, J. Camenisch, M. Dubovitskaya, A. Lysyanskaya, K. Samelin, L. Reyzin, **S. Yakoubov** (Euro S&P 2017)

Efficient Asynchronous Accumulators for Distributed PKI

L. Reyzin, **S. Yakoubov** (SCN 2016)

Cryptography for Big Data Security

A. Yerukhimovich, A. Hamlin, N. Schear, E. Shen, M. Varia, **S. Yakoubov** (2016)
This work appeared as a book chapter in "Big Data: Storage, Sharing, and Security".

Automated Assessment of Secure Search Systems

M. Varia, B. Price, N. Hwang, R. K. Cunningham, A. Hamlin, J. Herzog, J. Poland, M. Reschly, **S. Yakoubov** (ACM SIGOPS Operating Systems Review 2015)

HEtest: A Homomorphic Encryption Testing Framework

M. Varia, **S. Yakoubov**, Y. Yang (Workshop on Encrypted Computing and Applied Homomorphic Cryptography 2015)

A Survey of Cryptographic Approaches to Securing Big-Data Analytics in the Cloud

S. Yakoubov, V. Gadepally, N. Schear, E. Shen, A. Yerukhimovich (HPEC 2014)

Pattern Avoidance in Extensions of Comb-Like Posets

S. Yakoubov (Journal of Combinatorics 2015)
This work was also presented at Permutation Patterns 2013.

AWARDS

2016 MIT's Lincoln Scholars full scholarship and stipend for graduate Ph.D. work

2016 Aviation Week/AIAA 20 Twenties

2014 MIT's Lincoln Scholars full scholarship and stipend for graduate M.S. work

WORK EXPERIENCE

Spring 2017 Teaching Assistant, BU

Taught CS 558 (Network Security) discussion sections, and designed as well as oversaw applied cryptography labs.

Fall 2015 Teaching Assistant, BU

Held CS 538 (Cryptography) office hours and gave a substitute lecture for Professor Leo Reyzin.

Fall 2014 Grader, BU

Graded CS 538 (Cryptography) assignments for Professor Leo Reyzin.

2011–2019 Research Scientist, MIT Lincoln Laboratory

Lincoln Laboratory is a federally-funded research and development institution; while there, I worked on security-related projects for various branches of the US government.

- **Security and Privacy Assurance Research Program**. Worked as a researcher on developing auditing mechanisms (e.g. public verifiability) for secure computations.

- **Lincoln Laboratory Secure and Resilient Cloud**. Worked as a researcher and software developer on new techniques for secure multi-party computation with common practical applications.
- **Security and Privacy Assurance Research Program**. Worked as a researcher and software developer on the testing and evaluation of the SPAR program, which involves several research teams exploring new advances in somewhat homomorphic encryption and secure database search.
- **Cyber Red Blue**. Worked as a software developer on cyber simulation software. (Java)

Spring 2011 Grader, MIT

Graded 6.045 (Automata, Computability and Complexity) problem sets and exams for Professor Scott Aaronson.

January 2011 Undergraduate Researcher, MIT

Wrote code to test a few of Professor Shafi Goldwasser's new results (algorithms for canonically finding generators, and for canonically finding qth non-residues).

Summer 2010 Junior Software Engineer, W3C

- Worked for Sir Timothy Berners-Lee on the Tabulator, a generic data browser and editor which organizes information through RDF files.
- Designed and implemented user interfaces in JavaScript.

OTHER PROFESSIONAL EXPERIENCE

Ongoing Referee, Peer-Reviewed Publications

Reviewed papers for ACM CCS (Computer and Communications Security), ACNS (Applied Cryptography and Network Security), Crypto, Eurocrypt, ICITS (International Conference on Information Technology and Systems), ICML (International Conference on Machine Learning), ITCS (Innovations in Theoretical Computer Science), Journal of Combinatorics, PKC (Public Key Cryptography), RWC (Real World Crypto), SCN (Security and Cryptography for Networks), STOC (Symposium on Theory of Computing), TCC (Theory of Cryptography Conference), TOPS (Transactions on Privacy and Security)

2021 Program Committee Member, Asiacrypt

2021 Program Committee Member, ACM CCS

2020-2021 Committee Member, ALICE

(ALICE: Alliance for women in IT, Computing, and Engineering at Aarhus University)

2017 Committee Member, MASS AWIS

(MASS AWIS: Massachusetts Chapter of Association of Women in Science)

Winter 2017-18 Student Program Committee Member, IEEE S&P

Summer 2015, 2016, 2017, 2018, 2019 Volunteer, MIT Lincoln Laboratory

Designed, organized and taught LLCipher, a theoretical crypto summer program for high school students.

2017 Volunteer, MIT Lincoln Laboratory

Volunteered at Code Creative, a program that introduces high school students to computer science.

2013 Volunteer, MIT Lincoln Laboratory

Coached middle school children in building an autonomous Lego robot.

April 25, 2021