SOPHIA YAKOUBOV

ASSISTANT PROFESSOR, AARHUS UNIVERSITY

PERSONAL INFORMATION

email	sophia.yakoubov@cs.au.dk
website	http://web.mit.edu/sonka89/www/
address	Åbogade 34, 8200 Aarhus, Denmark
focus areas	Cryptography, Secure Computation

WORK EXPERIENCE

2021-Present	Assistant Prof. at Aarhus University, Denmark
2019-2021	Post-doc at Aarhus University, Denmark
2011-2019	Research Scientist at MIT Lincoln Lab, USA

EDUCATION

May 17, 2020	Ph.D. in Computer Science at Boston University Advised by Prof. Leo Reyzin
Jan 25, 2016	M.S. in Computer Science at Boston University
June 3, 2011	B.S. in Mathematics at MIT

AWARDS

2023	L'Oreal Women in Science Award
2016	MIT Lincoln Scholars Full scholarship and stipend for graduate Ph.D. work
2016	Aviation Week/AIAA 20 Twenties
2014	MIT Lincoln Scholars Full scholarship and stipend for graduate M.S. work

GRANTS

2022	Sapere Aude: DFF-Starting Grant YOSO: "You Only Speak Once" Secure Computation (DFF: Independent Research Fund Danmark)
2022	DIREC Explore Project Accountability and Privacy Preserving Computation on the Blockchain (DIREC: Digital Research Centre Danmark)
2021	DFF Project 1 Grant YOSO: "You Only Speak Once" Secure Computation

TEACHING

2022-present	Instructor for Cryptographic Protocol Theory Co-teach Cryptographic Protocol Theory, a Master's level course offered every Spring at Aarhus University.
2015-2019	Lead of the LLCipher Program Designed, organized and taught LLCipher, a theoretical crypto summer program for high school students, at MIT.

2017 TA for Network Security
Taught CS 558 (Network Security) discussion sections, and designed as well as oversaw applied cryptography labs at Boston University.

SUPERVISION

2024-Present Jure Sternad, PhD student at Aarhus U.

2021-Present Sebastian Kolby, PhD student at Aarhus U.

2019-Present Masters' and Bachelors' theses at Aarhus U.

VOLUNTEER WORK

Ongoing Reviewer
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)

Ongoing Program Committee Member
Eurocrypt 2025, Crypto 2024, SCN 2022, Eurocrypt 2022, Asiacrypt 2021, PPML Workshop 2021, CCS 2021

2020-2022 ALICE Committee Member
(ALICE: Alliance for women in IT, Computing, and Engineering at Aarhus University)

2017 MASS AWIS Committee Member
(MASS AWIS: Massachusetts Chapter of Association of Women in Science)

PUBLISHED PAPERS

1. Multi Designated Verifier Ring Signatures
   S. Kolby, E. Pagnin, **S. Yakoubov**; Communications in Cryptology 2024
2. Constant-Round YOSO MPC Without Setup
   S. Kolby, D. Ravi, **S. Yakoubov**; Communications in Cryptology 2024
3. Efficient Secure Communication Over Dynamic Incomplete Networks With Minimal Connectivity
   I. Damgård, D. Ravi, L. Roy, D. Tschudi, **S. Yakoubov**; TCC 2024
4. Broadcast-Optimal Two Round MPC with Asynchronous Peer-to-Peer Channels
   I. Damgård, D. Ravi, L. Siniscalchi, **S. Yakoubov**; Latincrypt 2023
5. Broadcast-Optimal Four-Round MPC in the Plain Model
   M. Chiampi, I. Damgård, D. Ravi, L. Siniscalchi, Y. Xia, **S. Yakoubov**; TCC 2023

6. Taming Adaptivity in YOSO Protocols: The Modular Way
   R. Canetti, S. Kolby, D. Ravi, E. Soria-Vazquez, **S. Yakoubov**; TCC 2023

7. Secure Communication in Dynamic Incomplete Networks
   I. Damgård, D. Ravi, D. Tschudi, **S. Yakoubov**; ITC 2023

8. Minimizing Setup in Broadcast-Optimal Two Round MPC
   I. Damgård, D. Ravi, L. Siniscalchi, **S. Yakoubov**; Eurocrypt 2023

9. Threshold-Optimal MPC with Friends and Foes
   N. Melissaris, D. Ravi, **S. Yakoubov**; Indocrypt 2023

10. The State of the Union: Union-Only Signatures for Data Aggregation
    D. Aranha, F. Engelmann, S. Kolby, **S. Yakoubov**; SCN 2022

11. On Sufficient Oracles for Secure Computation with Identifiable Abort
    M. Simkin, L. Siniscalchi, **S. Yakoubov**; SCN 2022

12. Distributed (Correlation) Samplers: How to Remove a Trusted Dealer in One Round
    D. Abram, P. Scholl, **S. Yakoubov**; Eurrocrypt 2022

13. Count Me In! Extendability for Threshold Ring Signatures
    D. F. Aranha, M. Hall-Andersen, A. Nitulescu, E. Pagnin, **S. Yakoubov**; PKC 2022

14. Random-index PIR and Applications
    C. Gentry, S. Halevi, B. Magri, J. B. Nielsen, **S. Yakoubov**; TCC 2021

15. Stronger Notions and a More Efficient Construction of Threshold Ring Signatures
    A. Munch-Hansen, C. Orlandi, **S. Yakoubov**; Latincrypt 2021

16. You Only Speak Once: Secure MPC with Stateless Ephemeral Roles
    C. Gentry, S. Halevi, H. Krawczyk, B. Magri, J. B. Nielsen, T. Rabin, **S. Yakoubov**; Crypto 2021

17. Broadcast-Optimal Two Round MPC with an Honest Majority
    I. Damgård, B. Magri, D. Ravi, L. Siniscalchi, **S. Yakoubov**; Crypto 2021

18. The Rise of Paillier: Homomorphic Secret Sharing and Public-Key Silent OT
    C. Orlandi, P. Scholl, **S. Yakoubov**; Eucrocrypt 2021

19. Broadcast Secret-Sharing, Bounds and Applications
    I. Damgård, K. Green-Larsen, **S. Yakoubov**; Information-Theoretic Cryptography (ITC) 2021

20. Turning HATE Into LOVE: Homomorphic Ad Hoc Threshold Encryption for Scalable MPC
    L. Reyzin, A. Smith, **S. Yakoubov**; CSCML 2021

21. Stronger Security and Constructions of Multi-Designated Verifier Signatures
    I. Damgård, H. Haagh, R. Mercer, A. Nitulescu, C. Orlandi, **S. Yakoubov**; TCC 2020

22. Universally Composable Accumulators
    R. Canetti, F. Baldimtsi, **S. Yakoubov**; CT-RSA 2020

23. Fuzzy Password-Authenticated Key Exchange
    P.A. Dupont, J. Hesse, D. Pointcheval, L. Reyzin, **S. Yakoubov**; Eurocrypt 2018

24. Catching MPC Cheaters: Identification and Openability
    R. Cunningham, B. Fuller, **S. Yakoubov**; ICITS 2017

25. 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

26. Efficient Asynchronous Accumulators for Distributed PKI
    L. Reyzin, **S. Yakoubov**; SCN 2016

27. Cryptography for Big Data Security
    A. Yerukhimovich, A. Hamlin, N. Schear, E. Shen, M. Varia, **S. Yakoubov**; Book chapter in "Big Data: Storage, Sharing, and Security", 2016

28. 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

29. HEtest: A Homomorphic Encryption Testing Framework
    M. Varia, **S. Yakoubov**, Y. Yang; Workshop on Encrypted Computing and Applied Homomorphic Cryptography 2015

30. 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

31. Pattern Avoidance in Extensions of Comb-Like Posets
    S. Yakoubov; Journal of Combinatorics 2015

September 25, 2024