CURRICULUM VITAE

29.02.2024

Personal Information

Name:	Janno Siim
Date of birth:	18.03.1992
Phone nr:	47 41297818
E-mail:	jannosiim@gmail.com
Web page	https://jannosiim.github.io/home/
DBLP	https://dblp.org/pid/209/1796.html
Google Scholar	https://scholar.google.com/citations?user=iA-LJYYAAAAJ&hl=en&oi=ao

EDUCATION

2016 - 2020	**PhD Degree in Computer Science** University of Tartu, Institute of Computer Science
2014 - 2016	**Master's Degree in Computer Science *(cum laude)*** University of Tartu, Faculty of Mathematics and Computer Science
2011- 2014	**Bachelor's Degree in Computer Science *(cum laude)*** University of Tartu, Faculty of Mathematics and Computer Science
2008 - 2011	Kuressaare Secondary School
1998 - 2008	Kaarma Primary School

EMPLOYMENT

2022 -	Postdoctoral Fellow, Simula UiB
2021 - 2022	Research Fellow in Cryptography, University of Tartu
2020 (6 months)	Research Associate, University of Edinburgh
2016 - 2020	Junior Research Fellow in Cryptography, University of Tartu
2019	Teaching assistant, University of Tartu Course: Cryptographic Protocols

2016 - 2018	Junior Researcher, Software Technology and Applications Competence Center (STACC)
2016	Research Project Specialist, University of Tartu
2015	Teaching assistant, University of Tartu
	Course: Algorithms and Data Structures
2014	Teaching assistant, University of Tartu
	Course: Elements of Discrete Mathematics

SKILLS

Languages	Estonian (Native language), English (excellent), Russian (beginner), German (beginner), Norwegian (beginner)
Programming	Some experience in C++, Java, Python, and several other languages.

RESEARCH INTERESTS

My main research interests are efficient cryptographic protocols and security assumptions. I have designed numerous efficient non-interactive zero-knowledge proofs (e.g., SNARKs) and different components for electronic voting protocols. My work has also focused on reducing trust assumptions in those protocols and making them rely on better-understood computational assumptions.

THESIS

1. PhD thesis, Non-Interactive Shuffle Arguments, 2020.
2. Master's thesis, Secure and Efficient Mix-Nets. 2016.

PUBLICATIONS

1. Helger Lipmaa, Roberto Parisella, **Janno Siim**. *Constant-Size zk-SNARKs in ROM from Falsifiable Assumptions.* To appear in Eurocrypt 2024.
2. Helger Lipmaa, Roberto Parisella, **Janno Siim**. *Algebraic Group Model with Oblivious Sampling.* In: Rothblum, G., Wee, H. (eds) Theory of Cryptography. TCC 2023. Lecture Notes in Computer Science, vol 14372. Springer, Cham.
3. Matteo Campanelli., Chaya Ganesh, Hamidreza Khoshakhlagh, **Janno Siim**. *Impossibilities in Succinct Arguments: Black-Box Extraction and More.* In: El Mrabet, N., De Feo, L., Duquesne, S. (eds) Progress in Cryptology - AFRICACRYPT 2023. AFRICACRYPT 2023. Lecture Notes in Computer Science, vol 14064. Springer, Cham.

4. Helger Lipmaa, **Janno Siim**, Michal Zajac. *Counting vampires: from univariate sumcheck to updatable ZK-SNARK*. In: Agrawal, S., Lin, D. (eds) Advances in Cryptology – ASIACRYPT 2022. ASIACRYPT 2022. Lecture Notes in Computer Science, vol 13792. Springer, Cham.
5. Markulf Kohlweiss, Mary Maller, **Janno Siim**, Mikhail Volkhov. *Snarky Ceremonies.* In: Tibouchi, M., Wang, H. (eds) Advances in Cryptology – ASIACRYPT 2021. ASIACRYPT 2021. Lecture Notes in Computer Science, vol 13092. Springer, Cham.
6. Prastudy Fauzi, Helger Lipmaa, **Janno Siim**, Michal Zajac, and Arne Tobias Ødegaard. *Verifiably-Extractable OWFs and Their Applications to Subversion Zero-Knowledge.* In: Tibouchi, M., Wang, H. (eds) Advances in Cryptology – ASIACRYPT 2021. ASIACRYPT 2021. Lecture Notes in Computer Science(), vol 13093. Springer, Cham.
7. Karim Baghery, Markulf Kohlweiss, **Janno Siim**, Mikhail Volkhov. *Another Look at Extraction and Randomization of Groth's zk-SNARK.* In: Borisov N., Diaz C. (eds) Financial Cryptography and Data Security. FC 2021. Lecture Notes in Computer Science, vol 12674. Springer, Berlin, Heidelberg.
8. Prastudy Fauzi , Helger Lipmaa, Zaira Pindado, **Janno Siim**. *Somewhere Statistically Binding Commitment Schemes with Applications.* In: Borisov N., Diaz C. (eds) Financial Cryptography and Data Security. FC 2021. Lecture Notes in Computer Science, vol 12674. Springer, Berlin, Heidelberg.
9. Behzad Abdolmaleki, Helger Lipmaa, **Janno Siim**, and Michal Zajac. *On Subversion-Resistant SNARKs.* Journal of Cryptology, Volume 34, Issue 3. Springer, 2021.
10. Behzad Abdolmaleki, Helger Lipmaa, **Janno Siim**, and Michal Zajac. *On QA-NIZK in the BPK Model.* In: PKC 2020, Part I. LNCS, volume 12110, pages 590-620.
11. Antonis Aggelakis, Prastudy Fauzi, Georgios Korfatis, Panos Louridas, Foteinos Mergoupis-Anagnou, **Janno Siim**, and Michal Zajac. *A Non-interactive Shuffle Argument With Low Trust Assumptions.* In CT-RSA 2020, LNCS, volume 12006, pages 667-692. Springer, Cham, 2020.
12. Behzad Abdolmaleki, Karim Baghery, Helger Lipmaa, **Janno Siim**, and Michal Zajac. *UC-secure CRS generation for SNARKs.* In AFRICACRYPT 19, LNCS, pages 99–117. Springer, Heidelberg, 2019.
13. Behzad Abdolmaleki, Karim Baghery, Helger Lipmaa, **Janno Siim**, and Michal Zajac. *DL-extractable UC-commitment Schemes.* In ACNS 19, LNCS, pages 385–405. Springer, Heidelberg, 2019.
14. Sven Heiberg, **Janno Siim**, Ivo Kubjas, Jan Willemson. *On Trade-offs of Applying Block Chains for Electronic Voting Bulletin Boards.* Proceedings of the Third International Joint Conference on Electronic Voting E-Vote-ID 2018: E-Vote-ID 2018, October 2-5, 2018, Bregenz, Austria. Ed. Robert Krimmer, Melanie Volkamer, Véronique Cortier, David Duenas-Cid, Rajeev Goré, Manik Hapsara, Reto Koenig, Steven Martin, Ronan McDermott, Peter Roenne, Uwe Serdült, Tomasz Truderung. TUT Press, 259-276.
15. Aggelos Kiayias, Annabell Kuldmaa, Helger Lipmaa, **Janno Siim**, and Thomas Zacharias. *On the Security Properties of E-voting Bulletin Boards.* In Dario Catalano and Roberto De Prisco, editors, SCN 18, volume 11035 of LNCS, pages 505–523. Springer, Heidelberg, September 2018.
16. Prastudy Fauzi, Helger Lipmaa**, Janno Siim**, and Michal Zajac. *An Efficient Pairing-based Shuffle Argument.* In Tsuyoshi Takagi and Thomas Peyrin, editors, ASIACRYPT 2017, Part II, volume 10625 of LNCS, pages 97–127. Springer, Heidelberg, December 2017.

17. Rein Prank, Heiki Pärn, **Janno Siim**. *Interactive Environment For Exercises In Graph Theory.* EDULEARN15 Proceedings: 7th International Conference on Education and New Learning Technologies, IATED, pages 4897−4905. July, 2015.

SIGNIFICANT PRESENTATIONS

Invited Talks:

1. Bergen central bank digital currency conference, 2022. Invited talk on privacy tools in distributed ledgers.

Conference Publication Presentations:

1. Eurocrypt 2024, Zurich, Switzerland. (Upcoming)
2. Africacrypt 2023, Sousse, Tunisia.
3. Asiacrypt 2022, Taipei, Taiwan.
4. Asiacrypt 2021, online.
5. Financial Cryptography and Data Security 2021, online.
6. Estonian-Latvian theory days 2018 and 2019. Presentations on various research results.
7. CT-RSA 2020, San Francisco, USA.
8. Africacrypt 2018, Rabat, Morocco.
9. SCN 2018, Amalfi, Italy.
10. Asiacrypt 2017, Hong Kong, China.
11. EDULEARN15, Barcelona, Spain.

COMMUNITY WORK

1. Eurocrypt 2023 Program committee member.
2. ACNS 2021 Program committee member.
3. 4th ZKProof Workshop (2021) - Standardization proposal for SNARK ceremonies (with Markulf Kohlweiss, Mary Maller, and Mikhail Volkhov)
4. Reviewing publications for various conferences and journals, including CRYPTO; Eurocrypt; Asiacrypt; PKC; Financial Cryptography; ACNS; Design, Codes, and Cryptography.

SUPERVISION

1. Shahla Atapoor. Master's thesis (2020). *On Privacy Preserving Blockchains and zk-SNARKs.* (Shahla continued as a PhD student in cryptography under the supervision of Nigel Smart in KU Leuven's COSIC research group, which is one of the best in the world.)
2. Marek Pagel (2017). Bachelor's thesis. *Performance Testing Bulletin Board Implementations for Online Voting.* (Marek is currently a senior software developer and tech lead in Bolt)