CYBERSECURITY
AND PRIVACY INSTITUTE
UNIVERSITY OF WATERLOO

Digital Overground

Cybersecurity and Privacy Institute Student Newsletter

For the February edition of Digital OverGround, we would like to take this opportunity to respectfully acknowledge Black History Month. While the representation of folx in the greater Black community working in cybersecurity is growing, a recent report states that they make up only 9 percent of the cyber workforce in America. People like Window Snyder, Christopher Young, Corey Thomas, Roy Clay, and Jerry Lawson have all contributed to our everyday lives with their work, we urge you to take a moment to read up on their individual contributions to our field.

If you are interested in contributing to this newsletter, please email us at CPI Students <cpi.students@uwaterloo.ca> we welcome the help!

Upcoming Events

Surveillance Capitalism: A Conversation with Shoshana Zuboff and Jim Balsillie

The Balsillie School of International Affairs (BSIA) and the Centre for International Governance Innovation (CIGI) are hosting a discussion on surveillance capitalism that features Shoshana Zuboff and Jim Balsillie on **Thursday, February 22, 2024, 4:00 PM – 5:30 PM**, with a reception to follow. This is a great academic and networking opportunity for students with an interest in surveillance, privacy, and public policy. Advance registration is required to attend.

Quantum Sensing Workshop Application
Friday, February 23, 2024

Velocity Presents - Startup 101: Grants & Non-dilutive Funding
Monday, February 26, 2024

Music Bingo at the Graduate House on Thursday, February 29, 2024, 6:00 PM
Participation is free and there will be prizes!

Masala Mocktail Night (SLC)
Tuesday, March 5, 2024

Fired Up at REV
Wednesday, March 6, 2024

South Side Marketplace Event (SCH)
Tuesday, March 26, 2024

Student Support and Resources

Campus Wellness and Counselling Services

CPI for Students

Current Students Pathways

CPI Undergraduate Award

CPI Excellence Graduate Scholarship

The Vector Digital Talent Hub

Research

From an Authentication Question to a Public Social Event: Characterizing Birthday Sharing on Twitter

Dilara Keküllüoğlu, Walid Magdy, CPI Member Kami Vaniea

Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data

Daniel J. Solove

The Poor Usability of OpenLDAP Access Control Lists

Yi Fei Chen, Rahul Punchhi, CPI Member Mahesh Tripunitara

Can I Borrow Your ATM? Using Virtual Reality for (Simulated) In Situ Authentication Research

Florian Mathis, CPI Member Kami Vaniea, Mohamed Khamis

PPR: Pairwise Program Reduction

Mengxiao Zhang, Zhenyang Xu, Yongqiang Tian, Yu Jiang, CPI Member Chengnian Sun

Open Calls

The Vector Digital Talent Hub encourages students to create profiles on their website to apply for a variety of employment opportunities. | Vector Institute

ICITST 2024 : International Conference for Internet Technology and Secured Transactions

The 40th Annual Qualitative Analysis Conference: 'Origin Stories:' Tracing the Origins of Ideas, Selves, and Communities

The 40th Annual Qualitative Analysis Conference will be held at Wilfrid Laurier University in Brantford, Ontario from June 26-28, 2024. This is a great opportunity for students conducting qualitative research in the areas of cybersecurity and privacy to share their work in front of an academic audience. The close conference location also makes this year's conference an optimal time for students with limited conference funding to present their work at an international conference. All stages of research are welcome (proposal, in progress, completed) and both paper and poster presentation options are available. **Abstracts are due by March 1, 2024.**

2024 American Society of Criminology Annual Meeting

The 2024 ASC Annual Meeting will be held at Marriott Marquis in San Francisco, CA from November 13-16, 2024. This year's theme is *Criminological Research and Education Matters: People, Policy, and Practice in Tumultuous Times*. Abstracts for thematic panels, individual papers, and author meets critic sessions are **due Friday, March 22, 2024.**

Abstracts for posters, roundtable sessions and lightning talks are due **Friday, May 17, 2024.**

In the Media

- **Podcast of the Month: Cybersecurity Today – This episode reports on advice for protecting water utilities from cyber attacks, Avast agrees to a settlement with FTC on allegations it wrongly sold consumer data**
- **'Facial recognition' error message on vending machine sparks concern at University of Waterloo**
- **Tor Code Audit Finds 17 Vulnerabilities**
- **Adobe Patches 207 Security Bugs in Mega Patch Tuesday Bundle**
- **New Google Initiative to Foster AI in Cybersecurity**
- **Tech Companies Sign Accord to Combat AI-Generated Election Trickery**
- **Apple Adds Post-Quantum Encryption to iMessage**
- **Threat Actors Quick to Abuse 'SSH-Snake' Worm-Like Tool**
- **You need to learn AI in 2024! (And here is your roadmap)**
- **FASTEST way to become a Cyber Security Engineer and ACTUALLY get a job**

Student Spotlights

CPI Members Dr. Adam Molnar and PhD Candidate Danielle Thompson presented their research at the Office of the Information Privacy Commissioner of Ontario in Toronto on February 15, 2024. Their presentation titled *Employee Monitoring in the Age of Remote Work: Insights from an Interdisciplinary Research Project* shared ongoing findings from a comprehensive research project into EMAs that is being undertaken in Canada and the UK. Specifically, drawing on data sets collected through computer science, legal, and social science methods, the presentation discussed:

- Survey data on current trends surrounding the use of EMAs in Canada.
- The security and privacy risks and vulnerabilities associated with the use of EMAs.
- Legal and regulatory challenges regarding the use of EMAs in Canada and the UK.

For further reading on their work, please see their paper:

[Workplace Surveillance in Canada: A survey on the adoption and use of employee monitoring applications]()

Seen anything that you think should be on this list for our next edition? Let us know!

CPI Students <cpi.students@uwaterloo.ca>

Speeding Up Multi-Scalar Multiplication over Fixed Points Towards Efficient zkSNARKs

Guiwen Luo, Shihui Fu and Guang Gong
{guiwen.luo, shihui.fu, ggong}@uwaterloo.ca
Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, CANADA

February’s student spotlight is from Guiwen Luo and Shihui Fu (ECE), with their work entitled: **Speeding Up Multi-Scalar Multiplication over Fixed Points Towards Efficient zkSNARKs**.

The arithmetic of computing multiple scalar multiplications in an elliptic curve group then adding them together is called multi-scalar multiplication (MSM). MSM over fixed points dominates the time consumption in the pairing-based trusted setup zero-knowledge succinct non-interactive argument of knowledge (zkSNARK), thus for practical applications we would appreciate fast algorithms to compute it. This paper proposes a bucket set construction that can be utilized in the context of Pippenger’s bucket method to speed up MSM over fixed points with the help of precomputation. If instantiating the proposed construction over BLS12-381 curve, when computing n-scalar multiplications for n = 2e (10 ≤ e ≤ 21), theoretical analysis indicates that the proposed construction saves more than 21% computational cost compared to Pippenger’s bucket method, and that it saves 2.6% to 9.6% computational cost compared to the most popular variant of Pippenger’s bucket method. Finally, our experimental result demonstrates the feasibility of accelerating the computation of MSM over fixed points using large precomputation tables as well as the effectiveness of our new construction.

Find Out More about Digital Overground

Our mailing address is:

200 University Ave W. DC 3147 Waterloo, Ontario N2L 3G1