Yevgeniy Vahlis

Curriculum Vitae

http://www.cs.toronto.edu/~evahlis evahlis@cs.toronto.edu

I Work Experience

October 2013–Present, Nymi Inc., Toronto, ON
Chief Cryptographer

July 2011–October 2013, AT&T Labs, New York, NY
Senior Researcher

- Member of the Security Research Center at AT&T Labs

July 2010–June 2011, Columbia University, New York, NY
Postdoctoral Research Scientist

- Member of the Cryptography Lab, Department of Computer Science

September 2009, Massachusetts Institute of Technology (MIT), Cambridge, MA
Visiting Ph.D. Student

II Education

University of Toronto, Toronto, ON, Canada
Ph.D. in Computer Science, August 2010
Thesis advisor: Charles Rackoff
Thesis: Black-Box and White-Box Cryptography

University of Toronto, Toronto, ON, Canada
M.Sc. in Computer Science, April 2007
Thesis advisor: Charles Rackoff
Thesis: Chosen-Ciphertext Security in Identity Based Encryption

Hebrew University of Jerusalem, Israel
B.Sc. in Computer Science (with a minor in Mathematics), June 2004

III Research Awards and Grants

- Natural Sciences and Engineering Research Council of Canada Postdoctoral Fellowship (NSERC), 2011–2013
- Alexander Graham Bell Canada Graduate Award (NSERC), 2009–2011.
- IARPA SPAR Program, February 2011. Initial proposal writer. Funding awarded to team: $2.23M.
- Hebrew University of Jerusalem, Dean's List, 2003

IV REFEREED PUBLICATIONS

1. Secure Key Exchange and Sessions Without Credentials. Ran Canetti, Vladimir Kolesnikov, Charles Rackoff, and Yevgeniy Vahlis. Security and Cryptography for Networks (SCN 2014). Springer International Publishing, 2014. 40–56.
2. EyeDecrypt-Private Interactions in Plain Sight. Andrea Forte, Juan Garay, Trevor Jim, and Yevgeniy Vahlis. Security and Cryptography for Networks (SCN 2014). Springer International Publishing, 2014. 255–276.
3. Efficient Network-Based Enforcement of Data Access Rights. Paul Giura, Vladimir Kolesnikov, Aris Tentes, and Yevgeniy Vahlis. Security and Cryptography for Networks (SCN 2014). Springer International Publishing, 2014. 236–254.
4. Is It Really You? User Identification via Adaptive Behavior Fingerprinting. Paul Giura, Ilona Murynets, Roger Piqueras Jover and Yevgeniy Vahlis. Fourth Conference on Data and Application Security and Privacy, ACM CODASPY 2014, 333–344.
5. Secure two-party computation in sublinear (amortized) time. Dov Gordon, Jonathan Katz, Vladimir Kolesnikov, Fernando Krell, Tal Malkin, Mariana Raykova, and Yevgeniy Vahlis. ACM CCS, 2012, 513–524.
6. Multi-location Leakage Resilient Cryptography. Ali Juma, Yevgeniy Vahlis, and Moti Yung. PKC, Springer, 2012, 7293, 504–521.
7. Verifiable Delegation of Computation over Large Datasets. Siavosh Benabbas, Rosario Gennaro, and Yevgeniy Vahlis. CRYPTO, Springer, 2011, 6841, 111–131.
8. Signatures Resilient to Continual Leakage on Memory and Computation. Tal Malkin, Isamu Teranishi, Yevgeniy Vahlis, and Moti Yung. TCC, 2011, 6597, 89–106 .
9. Protecting Cryptographic Keys against Continual Leakage. Ali Juma, and Yevgeniy Vahlis. CRYPTO, Springer, 2010, 6223, 41–58.
10. Two Is a Crowd? A Black-Box Separation of One-Wayness and Security under Correlated Inputs. Yevgeniy Vahlis. TCC, Springer, 2010, 5978, 165–182.
11. On the Impossibility of Basing Identity Based Encryption on Trapdoor Permutations FOCS. Dan Boneh, Periklis Papakonstantinou, Charles Rackoff, Yevgeniy Vahlis, Brent Waters. IEEE Computer Society, 2008, 283–292.
12. CCA2 Secure IBE: Standard Model Efficiency through Authenticated Symmetric Encryption. Eike Kiltz, and Yevgeniy Vahlis. CT-RSA, Springer, 2008, 4964, 221–238.

Manuscripts in Submission

13. On The Limits of The Decisional Diffie-Hellman Assumption. Charles Rackoff, Periklis Papakonstantinou, Yevgeniy Vahlis.

V Patents

1. With Andrea Forte. Augmented reality based privacy and decryption. US 20140164772 A1.
2. With Jeffrey Bickford, Mikhail Istomin. Method and apparatus for providing provably secure user input/output. US 20140006800 A1.
3. With Qi Shen, Andrea G. Forte, Paul Giura, Mikhail Istomin, Wei Wang. Verification service. US 8739247 B2.

VI Invited Talks and Conference Presentations

EyeDecrypt: Cryptography Optimized for Visualization

1. January 2013: AT&T Shannon Laboratories Seminar
2. June 2013: Workshop on Leakage, Tampering and Viruses, Warsaw, Poland

Verifiable Delegation of Computation over Large Datasets

3. August 2011: 30th Annual International Conference on Cryptology (CRYPTO)
4. April 2011: Columbia University Computer Science Seminar
5. March 2011: IBM Research Security and Cryptography Seminar
6. March 2011: Microsoft Research Redmond Security and Cryptography Seminar

Amortized Sublinear Secure Multi-party Computation

7. May 2011: AT&T Security Research Center Seminar
8. May 2011: Alcatel-Lucent Seminar

Secure Key Exchange and Sessions Without Credentials

9. September 2010: New York Crypto Day
10. January 2011: Workshop on Trends in Theoretical Cryptography, Beijing, China

On The Limits of DDH Hard Groups

11. January 2011: Workshop on Trends in Theoretical Cryptography, Beijing, China

Signatures Resilient to Continual Leakage on Memory and Computation

12. November 2010: University of Toronto Theory Seminar

Protecting Cryptographic Keys Against Continual Leakage

13. August 2010: Verifiable Computation Workshop, MIT
14. April 2010: New York University Cryptography Seminar
15. April 2010: Columbia University Theory Seminar
16. October 2009: MIT/Microsoft Research New England CIS Seminar
17. October 2009: The 2nd Eastern Great Lakes Theory of Computation Workshop
18. September 2009: Brown University Theory Seminar

Two Is A Crowd? A Black-Box Separation Of One-Wayness and Security Under Correlated Inputs

19. November 2010: New York University Cryptography Seminar

20. February 2010: 7th Theory of Cryptography Conference TCC 2010

On The Impossibility of Basing Identity Based Encryption on Trapdoor Permutations

21. October 2008: IEEE Symposium on the Foundations of Computer Science FOCS

CCA2 Secure IBE: Standard Model Efficiency through Authenticated Symmetric Encryption

22. April 2008: RSA Conference, Cryptographers Track

VII News Articles

- Bitcoin, Identity, and Decentralized Auctions, Huffington Post, May 28, 2014.

VIII Professional Activities

Program Committees

1. WAHC 2015: Third Annual Workshop on Applied Homomorphic Cryptography
2. INSCRYPT 2014: China International Conference on Information Security and Cryptology,
3. WAHC 2014: Second Annual Workshop on Applied Homomorphic Cryptography
4. PKC 2014: 17th International Conference on Practice and Theory in Public-Key Cryptography
5. WAHC 2013: First Annual Workshop on Applied Homomorphic Cryptography
6. INSCRYPT 2013: China International Conference on Information Security and Cryptology,
7. ESORICS 2013: European Symposium on Research in Computer Security
8. CSAW 2012: Cyber Security Competition
9. INSCRYPT 2012: China International Conference on Information Security and Cryptology,
10. ESORICS 2012: European Symposium on Research in Computer Security
11. CSAW 2011: Cyber Security Competition

Organizing Committees

- The 2013 DIMACS Workshop on Current Trends in Cryptology
  `http://dimacs.rutgers.edu/Workshops/Cryptology/`
- New York CryptoDay, July 2012

Conference Referee

- CCS: Conference on Computer and Communications Security
- CRYPTO: International Cryptology Conference
- DISC: International Symposium on Distributed Computing
- STOC: Symposium on Theory of Computing
- FOCS: Foundations of Computer Science
- TCC: Theoretical Cryptography Conference
- ICITS: International Conference on Information Theoretic Security