

PETER T. WILLIAMS, PH.D.

Computer Science Department
Stony Brook University
Stony Brook, NY 11794-4400

petertw@cs.stonybrook.edu
<http://www.cs.stonybrook.edu/~petertw/>
(347) 766-3697

Education

Ph.D. in Computer Science, Stony Brook University, 2012.

B.S. in Computer Science, Summa Cum Laude, Brandeis University, 2005.

Awards and Honors

Graduate Council Fellowship, Stony Brook University, 2006-2011.

Michtom Prize for Academic Excellence in Computer Science, Brandeis University, 2005.

Phi Beta Kappa, Brandeis University, 2005.

Teaching

Instructor for CSE 308 - Software Engineering, Spring 2010, Stony Brook University.

Misc. lectures for CSE 409 - Introduction to System Security, Stony Brook University.

Misc. lectures for CSE 508 - Network Security, Stony Brook University.

Employment

Research Assistant	Stony Brook University	2006-Present
Research Intern	IBM Research (T.J. Watson)	2007, 2010-2011
Web Developer	Brandeis University	2005-2006
Student Web Developer	Brandeis University	2002-2005
Research Assistant	Dartmouth Medical School	2001-2005

Theses

Ph.D. Dissertation at Stony Brook University: Oblivious Remote Data Access Made Practical. May 2012. Dissertation advisor: Radu Sion. Thesis Committee: Erez Zadok, Rob Johnson, Adrian Perrig, Moti Yung.

This dissertation introduces new mechanisms for practical private data access and oblivious transaction processing, as well as new trusted hardware designs. A space-time trade-off of client storage vs. efficiency is explored, then expanded to the additional dimensions of multiplicity of clients, the nature of the trusted computing base (hardware vs. software), and the degree of client data processing (access vs. transactions vs. computation). The results are orders of magnitude more efficient than existing work. Together, they bridge the gap between theoretical possibility and practical feasibility.

Undergraduate Senior Honors Thesis at Brandeis University: Design, Analysis, and Implementation of an Optimizing Compiler of JScheme to the JVM. May 2005. Advised by Tim Hickey.

This thesis implements a JScheme compiler, which generates natural and efficient Java, while preserving the full expressive power of Scheme. This is achieved through a combination of static type analysis and an efficient tail-recursion implementation. The result is Java code that can run (in many cases) orders of magnitude faster than the JScheme interpreter.

Publications

Peter Williams, Radu Sion. SR-ORAM: Single Round-trip Oblivious RAM. To appear in ACNS Industrial Track Proceedings, 2012.

We present the first single-round-trip polylogarithmic time Oblivious RAM requiring only logarithmic client storage. Taking only a single round trip to perform a query, SR-ORAM has a communication/computation cost of $O(\log n)$, with $O(\log^2 n \log \log n)$, and under 2 round trips, overall amortized per-query communication requirements.

Peter Williams, Radu Sion, Miroslava Sotakova. Practical Oblivious Outsourced Storage. ACM Transactions on Information and System Security TISSEC, 2011.

We introduce a new practical mechanism for remote data storage with access pattern privacy and correctness. A storage client can deploy this mechanism to issue encrypted reads, writes, and inserts to a potentially curious and malicious storage service provider, without revealing information or access patterns. We describe a practical system that can execute an unprecedented several queries per second on terabyte-plus databases while maintaining full computational privacy and correctness.

Peter Williams, Rick Boivie. CPU Support for Secure Executables. 4th International Conference on Trust and Trustworthy Computing TRUST 2011.

To protect software and data against vulnerabilities and malware, we describe simple extensions to the Power Architecture for running Secure Executables. By using a combination of cryptographic techniques and context labeling in the CPU, these Secure Executables are protected on disk, in memory, and through all stages of execution against malicious or compromised software, and other hardware.

Martin Franz, Peter Williams, Bogdan Carbutar, Stefan Katzenbeisser, Andreas Peter, Radu Sion and Miroslava Sotakova. Oblivious Outsourced Storage with Delegation. Financial Cryptography and Data Security Conference FC 2011.

We consider a scenario where multiple clients want to share data on a server, while hiding all access patterns. We propose here a first solution to this problem based on Oblivious RAM (ORAM) techniques. Data owners can delegate rights to external new clients enabling them to privately access portions of the outsourced data served by a curious server.

Peter Williams, Radu Sion, Dennis Shasha. The Blind Stone Tablet: Outsourcing Durability. Network and Distributed System Security Symposium NDSS 2009. (acceptance rate: 11.7%)

We introduce a new paradigm for outsourcing the durability property of a multi-client transactional database to an untrusted service provider. Specifically, we enable untrusted service providers to support transaction serialization, backup and recovery for clients, with full data confidentiality and correctness. Moreover, providers learn nothing about transactions (except their size and timing), thus achieving read and write access pattern privacy.

Peter Williams, Radu Sion, Bogdan Carbutar. Building Castles out of Mud: Practical Access Pattern Privacy and Correctness on Untrusted Storage. ACM Conference on Computer and Communications Security CCS 2008. (acceptance rate: 18.1%)

We introduce a new practical mechanism for remote data storage with efficient access pattern privacy and correctness. We built a first practical system—orders of magnitude faster than existing implementations—that can execute over several queries per second on 1Tbyte+ databases with full computational privacy and correctness.

Peter Williams, Radu Sion. Usable PIR. Network and Distributed System Security Symposium NDSS 2008. (acceptance rate: 17.8%)

In the presence of a small amount ($O(\sqrt{n})$, where n is the size of the database) of temporary storage, we show that clients can achieve access pattern privacy with communication and computational complexities of less than $O(\log^2 n)$ per query. We achieve these novel results by applying new insights based on probabilistic analyses of data shuffling algorithms to Oblivious RAM, allowing us to significantly improve its asymptotic complexity.

Ambros V, Lee RC, Lavanway A, Williams PT, Jewell D. MicroRNAs and Other Tiny Endogenous RNAs in *C. elegans*. *Curr Biol* 2003 May 13; 13(10):807-18.

*MicroRNAs (miRNAs) are small noncoding RNAs that are processed from hairpin precursor transcripts by Dicer. miRNAs probably inhibit translation of mRNAs via imprecise antisense base-pairing. We employed cDNA sequencing and comparative genomics to identify additional *C. elegans* small RNAs with properties similar to miRNAs and siRNAs. We found three broad classes of small RNAs in *C. elegans*; these results suggest that diverse modes of small RNA-mediated gene regulation are deployed in normal worms.*

Selected Research Projects

Browser Isolation with MicroDomains: By viewing every site in a separate virtual machine, the browser's same-origin security policy is enforced externally; security flaws in the web browser are rendered harmless. (IBM Research)

Network Secure Searchable Storage with Privacy and Correctness: Efficient data outsourcing to an untrusted service provider, offering full read/write privacy and correctness. (Stony Brook)

Network Services Restructuring. Redesign the internal information paths of the Brandeis IT department to support an XML-RPC interface, allowing better application interoperability, administration, and data consistency. (Brandeis University)

MicroRNAs and Other Tiny Endogenous RNAs in *C. elegans*. Use a computational genetics approach, aggregating information from multiple sources (pattern matching, free energy calculations, and evolutionary data) to predict and validate candidate microRNAs. (Dartmouth Medical School)

Professional Activities

Program Committee member for the 2012 Network and Distributed System Security Symposium (NDSS).

Program Committee member for the 2009 Cloud Computing Security Workshop at CCS (CCSW).

Invited reviews for IEEE S&P (2012), SODA (2011), ICDCS (2011), JSS (2010), TCDE (2010), CCS (2008, 2007), IJIS (2008), TISSEC (2007).