Alex J. Malozemoff

November 8, 2016

Contact Information

University of Maryland
Department of Computer Science
A.V. Williams Building
College Park, MD 20742

http://www.cs.umd.edu/~amaloz
amaloz@galois.com

Research Interests

Cryptography · Computer Security

Education

University of Maryland, College Park, MD

Ph.D. Candidate: Computer Science — **2011 – 2016**
Master of Science: Computer Science — **2011 – 2013**
Advisor: Prof. Jonathan Katz
GPA: 4.0 / 4.0

McGill University, Montreal, QC, Canada

Bachelor of Science: Honors Computer Science — **2005 – 2010**
Minors: Mathematics, Music Technology
GPA: 3.97 / 4.0

- Transferred from *Bachelor of Music: Honors Music Technology* (McGill 2005 – 2007)

Phillips Academy, Andover, MA — **2001 – 2005**

Work Experience

Galois, Portland, OR
Research Lead — **07/2016 – present**

University of Maryland, College Park, MD
Department of Computer Science
Graduate Research Assistant — **08/2011 – 05/2016**

Bell Labs, Murray Hill, NJ
Intern — **01/2015 – 03/2015**

IDA/CCS, Bowie, MD
Summer Intern — **06/2013 – 08/2013**

U.S. Department of Defense
Summer Intern — **05/2012 – 08/2012**

Pacific Northwest National Laboratory, Richland, WA
Secure Cyber Systems, National Security Directorate
Ph.D. Intern — **08/2011 – 05/2012**
Post-Bachelor Research Associate — **07/2010 – 07/2011**

Argonne National Laboratory, Argonne, IL
Mathematics and Computer Science Division
Research Assistant — **05/2009 – 07/2009**

Work Experience (Continued)

McGill University, Montreal, QC, Canada
School of Computer Science
Research Assistant **05/2008 – 08/2008**

Fidelity Investments, Boston, MA
Unix System Administration Intern **05/2007 – 08/2007**

McGill University, Montreal, QC, Canada
Music Technology Department
Summer Intern **05/2006 – 08/2006**

Teaching Experience

McGill University, Montreal, QC, Canada
School of Computer Science
Teaching Assistant: COMP 302 — Programming Languages and Paradigms **Winter 2010**
Teaching Assistant: COMP 535 — Computer Networking **Fall 2008**, **Fall 2009**

Journal Publications

1. D. Apon, J. Katz, **A.J. Malozemoff**. One-round multi-party communication complexity of distinguishing sums. *Theoretical Computer Science*, 501:101–108, 2013.

Refereed Publications

1. K. Lewi, **A.J. Malozemoff**, D. Apon, B. Carmer, A. Foltzer, D. Wagner, D.W. Archer, D. Boneh, J. Katz, M. Raykova. "5Gen: A framework for prototyping applications using multilinear maps and matrix branching programs." *ACM CCS*, Vienna, Austria, October 24 – 28, 2016.
2. V. Kolesnikov, H. Krawczyk, Y. Lindell, **A.J. Malozemoff**, T. Rabin. "Attribute-based key exchange with general policies." *ACM CCS*, Vienna, Austria, October 24 – 28, 2016.
3. V. Kolesnikov, **A.J. Malozemoff**. "Public verifiability in the covert model (almost) for free." *Asiacrypt*, Auckland, New Zealand, November 29 – December 3, 2015.
4. V.T. Hoang, J. Katz, **A.J. Malozemoff**. "Automated analysis and synthesis of authenticated encryption schemes." *ACM CCS*, Denver, CO, USA, October 12–16, 2015.
   Recipient of the **Best Paper Award**.
5. Y. Huang, J. Katz, V. Kolesnikov, R. Kumaresan, **A.J. Malozemoff**. "Amortizing garbled circuits." *Crypto*, Santa Barbara, CA, USA, August 17–21, 2014.
6. S.G. Choi, J. Katz, **A.J. Malozemoff**, V. Zikas. "Efficient three-party computation from cut-and-choose." *Crypto*, Santa Barbara, CA, USA, August 17–21, 2014.
7. **A.J. Malozemoff**, J. Katz, M.D. Green. "Automated analysis and synthesis of block-cipher modes of operation." *IEEE Computer Security Foundations Symposium*, Vienna, Austria, July 19–22, 2014.

Honors & Awards

National Defense Science and Engineering Graduate Fellowship **2012 – 2015**

University of Maryland, College Park, MD
Dean's Fellowship **2011 – 2013**

Pacific Northwest National Laboratory, Richland, WA
Outstanding Performance Award **July 2011**

McGill University, Montreal, QC, Canada

Dean's Honor List	**2005 – 2010**
Arthur and Crystal Lau Scholarship	**2009 – 2010**
James McGill Award	**2008 – 2009**
Emily Crawford Scholarship	**2008 – 2009**
Schulich Scholar	**2007 – 2008**
McConnell Award	**2006 – 2007**
E & A Rossinger Scholarship	**2006 – 2007**

PROGRAMMING C, OCaml, Python

SERVICE **Reviewer:** IET Information Security; Transactions on Information Forensics & Security; Journal of Automated Reasoning; Asiacrypt (2014, 2015, 2016); ACNS (2015); CANS (2012); CCS (2014, 2016); Crypto (2014, 2016); Eurocrypt (2016); PKC (2012, 2014, 2016); TCC (2016-B); USENIX Security (2014)

OTHER U.S. Citizen