

Deian Stefan

The Cooper Union
41 Cooper Square, Room 725
New York, NY 10003

☎ 212-353-4023 or 646-355-8821

stefan@cooper.edu

www.ee.cooper.edu/~stefan or deian.net

Citizenship: US

Education

The Cooper Union for the Advancement of Science and Art

New York, NY

Master of Engineering in Electrical Engineering [GPA: 4.0/4.0]

August 2009 - May 2010 (expected)

- Full-tuition fellowship 2009-2010
- Minor: Computer Science
- Thesis: *Cryptanalysis of CubeHash, BLAKE and MICKEY 128 2.0*
- Selected Graduate Coursework: Compiler Theory, Adv. Computer Architecture, DSP System Design, Probability & Stochastic Processes, Operating Systems, Computer Security, Adv. Cryptography, Machine Learning, Adv. Embedded Systems, Wireless Communications, Sel. Topics in Number Theory, Compression and Information Theory

The Cooper Union for the Advancement of Science and Art

New York, NY

Bachelor of Engineering in Electrical Engineering [GPA: 3.7/4.0]










August 2005 - May 2009

- Full-tuition scholarship 2005-2009
- Track: Computer Engineering
- Senior Project: *WiSO Safe - A Sustainable Wireless Sensor Network to Detect Coastal Rip Currents*

Publications

deian.net/pubs/

Peer-reviewed Conferences/Workshops

1.  D. A. Osvik, J. W. Bos, D. Stefan, and D. Canright. Fast software AES encryption. In *International Workshop on Fast Software Encryption, FSE*, LNCS. Springer, 2010. Accepted.
2.  D. Stefan, I. L. Dalal, M. Sandora, C. Yu, N. Chitrik, S. Srinivasan, and K. Chatterjee. A parallelized quasi-monte carlo algorithm for the extraction of partial inductances in IC interconnect structures. In *Annual Review of Progress in Applied Computational Electromagnetics*. ACES, April 2010. Accepted.
3.  D. Stefan. Hardware framework for the Rabbit stream cipher. In *Inscrypt 2009*, LNCS. Springer, December 2009.
4.  H. Xiong, P. Malhotra, D. Stefan, C. Wu, and D. Yao. User-assisted host-based detection of outbound malware traffic. In *International Conference on Information and Communications Security, ICICS*, December 2009.
5.  J. W. Bos, D. A. Osvik, and D. Stefan. Fast implementations of AES on various platforms. In *Software Performance Enhancement for Encryption and Decryption and Cryptographic Compilers, SPEED-CC*, pages 19–24, October 2009.
6.  H. Edrees, B. Cheung, M. Sandora, D. B. Nummy, and D. Stefan. Hardware-optimized ziggurat algorithm for high-speed gaussian random number generators. In *International Conference on Engineering of Reconfigurable Systems & Algorithms, ERSA*, pages 254–260, July 2009.
7.  J. Harwayne-Gidansky, D. Stefan, and I. L. Dalal. FPGA-based SoC for real-time network intrusion detection using counting bloom filters. In *Southeastcon, 2009*, pages 452–458. IEEE, March 2009.
8.  I. L. Dalal, D. Stefan, and J. Harwayne-Gidansky. Low discrepancy sequences for monte carlo simulations on reconfigurable platforms. In *International Conference on Application-Specific Systems, Architectures and Processors, ASAP*, pages 108–113, July 2008.
9.  D. Stefan, D. B. Nummy, J. Harwayne-Gidansky, and I. L. Dalal. On parallelizing the CryptMT stream cipher. In *Vehicular Technology Conference, VTC Spring*, pages 1082–1086. IEEE, May 2008.

10. I. L. Dalal and D. Stefan. A hardware framework for the fast generation of multiple long-period random number streams. In *Proceedings of the ACM/SIGDA 16th International Symposium on Field Programmable Gate Arrays, FPGA*, pages 245–254. ACM, February 2008.
11. D. Stefan and C. Mitchell. On the parallelization of the MICKEY-128 2.0 stream cipher. In *The State of the Art of Stream Ciphers, SASC 2008*, pages 175–185, February 2008. Online proceedings at <http://www.ecrypt.eu.org/stv1/sasc2008/>.

Journals

1. K. Chatterjee, M. Sandora, C. Mitchell, D. Stefan, D. Nummey, and J. Poggie. A new software and hardware parallelized floating random-walk algorithm for the modified Helmholtz equation subject to Neumann and mixed boundary conditions. *Applied Computational Electromagnetics Society Journal*, March 2010. Accepted.
2. D. Stefan. Prostate ultrasound image processing. *Crossroads*, 13(3):20–23, March 2007.

Posters/Abstracts

1. D. Stefan, C. Wu, D. Yao, and G. Xu. Ensuring host integrity with cryptographic provenance verification. ACM Conference on Computer and Communications Security, ACM CCS, Poster Session, November 2009.
2. D. Stefan. Reconfigurable hardware implementations of the Rabbit stream cipher. Workshop on Cryptographic Hardware and Embedded Systems, CHES, Poster Session, September 2009.
3. D. Stefan, C. Wu, D. Yao, and G. Xu. Trusted-input for anomaly detection of botnets. The Third Annual DHS University Network Summit, March 2009. Poster.
4. K. Chatterjee, I. L. Dalal, D. S. C. Yu, N. Chitrik, M. Sandora, S. Srinivasan, and J. Poggie. A quasi-monte carlo solver for partial inductances in IC interconnect structures. In *Progress in Electromagnetics Research Symposium, PIERS*, July 2008. Abstract.

Talks

1. J. W. Bos, A. K. Lenstra, and D. Stefan. Accelerating cryptographic applications and attacks with multi-core game processors. Parallel Crypto Minisymposium, 2010 SIAM Conference on Parallel Processing and Scientific Computing, February 2010.

Patents

1. D. Yao, D. Stefan, and C. Wu. Robust Keystroke Authentication and Input-Traffic Correlation Analysis For Accurate Bot Detection. Provisional Patent Filed. Rutgers University, March 2009.

Research Experience

deian.net/research/

S*ProCom² – Cooper Union Center for Sig. Proc. Research

New York, NY

Graduate Research Fellow (Supervisor: Fred L. Fontaine)

September 2009 - Present

- ▶ Implement low-power and low-resource AES on FPGAs.
- ▶ Cryptanalysis of CubeHash and BLAKE using linear differential methods.
- ▶ Analysis of CubeAttack on MICKEY 128 2.0.
- ▶ Develop algebraic attacks on FPGA-based network intrusion detection systems.
- ▶ Implement eSTREAM portfolio and bitsliced Serpent on GPUs and Cell B.E.

LACAL – Ecole Polytechnique Fédérale de Lausanne

Lausanne, Switzerland

Summer Research Fellow (Supervisor: Arjen K. Lenstra)

June 2009 - September 2009

- ▶ Implement the AES for multi-stream high speed applications using GPUs.
- ▶ Implemented small code-size SHA-256 and SHA-512 on the AVR.
- ▶ Implemented SHA-3 candidates on GPUs.

- ▶ Cryptanalyzed of CubeHash using linear differential methods.
- ▶ Designed hardware framework for the Rabbit stream cipher.

DyDAn – Rutgers University

New Brunswick, NJ

Research Fellow (Supervisor: Danfeng Yao)

August 2008 - February 2009

- ▶ Applied machine learning methods (Dynamic Bayesian Networks, SVM, NN) to security problems.
- ▶ Studied stochastic modeling of user browsing patterns to detect anomalies.
- ▶ Wrote code for network traffic analysis.
- ▶ Designed and implemented a TPM-based trust agent as a Linux kernel module.

DIMACS

New Brunswick, NJ

REU Research Fellow (Supervisor: Danfeng Yao)

May 2008 - August 2008

- ▶ Studied botnets and botnet detection methods.
- ▶ Designed and implemented a host-based botnet/intrusion detection method based on keystroke dynamics.
- ▶ Studied classification and novelty detection methods for small number of training instances.
- ▶ Gave seminars on host-based botnet detection.

S*ProCom² – Cooper Union Center for Sig. Proc. Research

New York, NY

Senior Research Fellow (Supervisors: Fred L. Fontaine, Kausik Chatterjee)

July 2007 - September 2009

- ▶ Developed mathematical methods for optimizing the MICKEY 128 2.0 stream cipher.
- ▶ Designed and implementing parallel architectures for uniform and non-uniform random number generators.
- ▶ Studied supervised learning methods as applied to automated detection of failures in micro-vascular surgery.
- ▶ Developed a parallel framework for Monte Carlo simulations.
- ▶ Principal investigator on Navy STTR proposal (topic N09-T37) with MaXentric Technologies LLC.

Stevens Institute of Technology

Hoboken, NJ

NSF REU Research Fellow (Supervisors: Yu-Dong Yao, Hong Man)

May 2006 - July 2006

- ▶ Studied image processing techniques as applied to medical imaging.
- ▶ Implemented algorithms that autonomously determine the body of a prostate in ultrasound images.
- ▶ Gave a seminar on digital image processing using MATLAB.

Teaching Experience

Java Programming

New York, NY

Instructor (Bnai Zion and Cooper Union Immigrant Engineering Retraining Program)

Spring 2010

- ▶ Developing course curriculum on Java programming.
- ▶ Creating hands-on laboratory exercises for distributed application programming using Java.

ECE491 - Monte Carlo Methods

New York, NY

Teaching Assistant (for Prof. K. Chatterjee, The Cooper Union)

Spring 2009

- ▶ Created lecture plans and assignments on practical scientific programming.
- ▶ Gave lectures on high-performance computing using clusters (MPI), FPGAs, and GPGPUs.
- ▶ Assisted students with project implementations.

ECE150 - Digital Logic Design

New York, NY

Teaching Assistant (for Prof. K. Chatterjee, The Cooper Union)

Fall 2006, Spring 2007

- ▶ Gave lectures on simple programmable logic devices – PLDs, GALs.
- ▶ Assisted students with implementations of logic circuits.
- ▶ Wrote student manual on ABEL.

Work Experience

μ Lab – Cooper Union

New York, NY

Head Network Administrator

August 2005 - May 2008

- ▶ Administer GNU/Linux–based servers for the Electrical Engineering Dept. (DHCP, DNS, www, etc.).
- ▶ Install and maintain network license server and client software–(Cadence, Synopsys, Mentor Graphics, etc.).
- ▶ Maintain the hardware and software of over 50 lab computers.

EasyPixel

New York, NY

Founder and Web Developer

August 2002 - August 2004

- ▶ Started and managed a hosting and web development company (clients include: Harvard Rugby Club, No Stamp Mail, Inc., NY Hi-Tech Interiors, Inc.).
- ▶ Wrote front-end and back-end applications using Perl/CGI, MySQL, HTML, and PHP.
- ▶ Provided IT support and consulting.

Other Projects

deian.net/projects/

- **MICKEY-v2-bitlice:** Open source bitslice implementation of the MICKEY 2.0 stream cipher.
- **Crayon OS:** A small real-time operating system for the Power PC 405 on the ML403 development board.
- **SFCC:** A C compiler generating IR.
- **YASTL:** A small coarse grained user-level threads library.
- **dVoiceMail:** An open source voicemail system based on Asterisk.
- **xtrapdei:** An open source X11 user-space key logger.

Skills

- **Programming Languages:** C, C++, Perl, Python, PHP, lush, nesC, Lua, Bash, Cryptol
- **Notable Software/Libraries:** CUDA, OpenCL, Mathematica, MATLAB, Asterisk, Pthreads, MPI, OpenGL, GTK, WEKA, RapidMiner, L^AT_EX, PARI/GP, GAP, bison, flex, ncurses, openssl, TrouSerS
- **Embedded/FPGAs:** x86, ARM, AVR, Cell B.E., nVidia PTX, Verilog, VHDL, Xilinx *ISE* and *System Generator*, SynplifyPro/Premiere
- **Operating Systems:** GNU/Linux, *BSD, Mac OS X, Open Solaris, Windows XP/2003
- **Languages:** English, Romanian, Serbo-Croatian

Awards and Honors

- Graduated with Magna Cum Laude, May 2009.
- DIMACS botnet biometrics work featured in NSF Highlights, January 2009.
- 2nd Prize: I. L. Dalal and D. Stefan. A Parallel Framework for Long-period Random Number Generators in Hardware. European Workshop on Microelectronics Education (M.Sc. Track). Budapest, Hungary, May 2008.
- 2nd Prize: I. Dalal, J. Harwayne-Gidansky, and D. Stefan. On the Fast Generation of Long-period Pseudorandom Number Sequences. IEEE Region 1 Graduate Student Paper Contest. Farmingdale, NY, May 2008.
- 2nd Prize: J. Harwayne-Gidansky and D. Stefan. On the Fast Generation of Long-period Pseudorandom Number Sequences. IEEE Region 1 Student Conference, Teaneck, NJ, April 2008.
- Outstanding Summer Research Award. Stevens Institute of Technology ECE Department, July 2006.
- Honor societies: Tau Beta Pi, Eta Kappa Nu, Sigma Xi.

- Dean's List: Fall 2005, Spring 2006, Fall 2007, Spring 2008, Fall 2008, Spring 2009, Fall 2009.

Activities

- Professional societies: IACR, ACM, ACM SIGACT, IEEE, IEEE Computer Society.
- Journal reviewer: Computers & Electrical Engineering Journal, IEEE Potentials.
- Conference reviewer: IEEE VTC Fall 2008, IMACC'09.
- ACM Greater New York Regional Collegiate Programming Contest. Participant 2004, 2005, 2006.
- NYU-Poly Cyber Security Awareness Week. Hacking embedded crypto-communication device finalist, 2008.
- Contributing open source programmer on SourceForge.net and CPAN.org, 2007-Present.

References

Arjen K. Lenstra

Professor, Lab Director
Laboratory for Cryptologic Algorithms
Ecole Polytechnique Fédérale de Lausanne
INJ 330, Station 14
CH-1015 Lausanne, Switzerland
Tel: + 41 21 693 8101
akl@epfl.ch

Danfeng Yao

Assistant Professor
Department of Computer Science
Rutgers, the State University of New Jersey
110 Frelinghuysen Road
Piscataway, NJ 08854
Tel: 732 445 2001 ext. 1188
danfeng@cs.rutgers.edu

Fred L. Fontaine

Professor, Dept. Chairman
Department of Electrical Engineering
The Cooper Union for the Advancement of Science and Art
41 Cooper Square
New York, NY 10003
Tel: 212 353 4331
fred@cooper.edu

Kausik Chatterjee

Professor
Department of Electrical Engineering
The Cooper Union for the Advancement of Science and Art
41 Cooper Square
New York, NY 10003
Tel: 212 353 4333
chatte@cooper.edu

Additional references available upon request.

GPG Fingerprint

AD46 8E3C 093A 23C9 F73D C518 1E30 1775 531A A172

Last modified: February 1, 2010