

## 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

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

New York, NY

August 2009 - May 2010 (expected)

- Full-tuition fellowship 2009-2010
- Minor: Computer Science
- Thesis: *Cryptanalysis of CubeHash, BLAKE and MICKEY 128 2.0*

### The Cooper Union for the Advancement of Science and Art

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

New York, NY












August 2005 - May 2009

- Full-tuition scholarship 2005-2009
- Track: Computer Engineering


## Publications

[deian.net/pubs/](http://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. Nummey, 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. Nummey, 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/](http://deian.net/research/)

### **S\*ProCom<sup>2</sup> – Cooper Union Center for Sig. Proc. Research**

*Graduate Research Fellow* (Supervisor: Fred L. Fontaine)

New York, NY

*September 2009 - Present*

### **LACAL – Ecole Polytechnique Fédérale de Lausanne**

*Summer Research Fellow* (Supervisor: Arjen K. Lenstra)

Lausanne, Switzerland

*June 2009 - September 2009*

### **DyDAn – Rutgers University**

*Research Fellow* (Supervisor: Danfeng Yao)

New Brunswick, NJ

*August 2008 - February 2009*

### **DIMACS**

*REU Research Fellow* (Supervisor: Danfeng Yao)

New Brunswick, NJ

*May 2008 - August 2008*

### **S\*ProCom<sup>2</sup> – Cooper Union Center for Sig. Proc. Research**

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

New York, NY

*July 2007 - September 2009*

### **Stevens Institute of Technology**

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

Hoboken, NJ

*May 2006 - July 2006*

## Teaching Experience

### **Java Programming**

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

New York, NY

*Spring 2010*

### **ECE491 - Monte Carlo Methods**

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

New York, NY

*Spring 2009*

## ECE150 - Digital Logic Design

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

New York, NY

Fall 2006, Spring 2007

## Work Experience

### $\mu$ Lab – Cooper Union

Head Network Administrator

New York, NY

August 2005 - May 2008

### EasyPixel

Founder and Web Developer

New York, NY

August 2002 - August 2004

## Skills

- **Programming Languages:** C, C++, Perl, Python, PHP, lsh, nesC, Lua, Bash, Cryptol
- **Notable Software/Libraries:** CUDA, OpenCL, Mathematica, MATLAB, Asterisk, Pthreads, MPI, OpenGL, GTK, WEKA, RapidMiner, L<sup>A</sup>T<sub>E</sub>X, 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*, Synplify*Pro/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*