# John R. Black, Jr.

Department of Computer Science
430 UCB
University of Colorado
Boulder, CO 80309-0430  USA

| office: | +1 303 492-0573 |
| FAX: | +1 303 492-2844 |
| secretary: | +1 303 492-7514 |

Email:   `jrblack@cs.colorado.edu`
WWW:   `http://www.cs.colorado.edu/~jrblack/`

---

| **Position** | Assoc. Prof. Computer Science, University of Colorado at Boulder | *7/08–present* |
| | Vice President of Education, SecureSet LLC | *9/15–present* |

**Research**   Cryptography, Network Security, Computer Security.

| **Past Employment** | **University of Colorado at Boulder** | *7/02–7/08* |
| | Assistant Professor of Computer Science. | |
| | **University of Nevada, Reno** | *7/00–6/02* |
| | Assistant Professor of Computer Science. | |
| | **University of California, Davis** | *7/97–7/00* |
| | Research Assistant | |
| | **University of California, Davis** | *8/95–6/97* |
| | Teaching Assistant | |
| | **Ingres Corporation** | *6/88–4/94* |
| | Senior Member of Technical Staff | |

**Education**

**University of California, Davis**    *9/95–9/00*
Ph.D. in Computer Science.
Thesis: Message Authentication Codes.
Advisor: Phillip Rogaway.

**California State University at Hayward**    *9/84–6/88*
B.S. in Computer Science and Mathematics, 1988.
Honors: Summa Cum Laude

**Awards**

NSF CAREER Award, 2002
Chancellor's Teaching Fellowship, UC Davis, 1998
Outstanding Teaching Assistant, UC Davis, 1998
Outstanding Teaching Assistant, UC Davis, 1997
A Check for $2.56 from Don Knuth, 1996

**Journal Publications**

**1**. P. Rogaway, M. Bellare and J. Black, "OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption." *ACM Transactions on Information and System Security (TISSEC)*, Volume 6, Issue 3, pp. 365–403, August, 2003.

**2**. J. Black, and P. Rogaway, "CBC MACs for Arbitrary Length Messages: The Three-Key Constructions." *Journal of Cryptology*, Volume 18, Number 2, pp. 111–132, Spring, 2005.

**3**. J. Black, "The Impossibility of Technology-Based DRM and a Modest Suggestion." *Journal of Telecommunications and High-Technology Law —JTHTL*, Volume 3, Number 2, pp. 387–396, Spring, 2005.

**4**. J. Black, M. Cochran and R. Gardner, "An Analysis of the Internet Chess Club." *IEEE Security and Privacy*, Volume 4, Number 1, pp. 46–52, January, 2006.

**5**. J. Black, M. Cochran and T. Shrimpton, "On the Impossibility of Highly-Efficient Blockcipher-Based Hash Functions." *Journal of Cryptology*, Volume 22, Number 3, pp. 311–329, Fall, 2009.

**6**. J. Black, P. Rogaway, T. Shrimpton, and M. Stam "An Analysis of the Blockcipher-Based Hash Functions from PGV." *Journal of Cryptology*, Volume 23, Number 4, pp. 519–545, Fall, 2010.

**7**. C. Wilks, M. Cline, E. Weiler, M. Diehkans, B. Craft, C. Martin, D. Murphy, H. Pierce, J. Black, D. Nelson, B. Litzinger, T. Hatton, L. Maltbie, M. Ainsworth, P. Allen, L. Rosewood, E. Mitchell, B. Smith, J. Warner, J. Groboske, H. Telc, D. Wilson, B. Sanford, H. Schmidt, D. Haussler, D. Maltbie "The Cancer Genomics Hub (CGHub): overcoming cancer through the power of torrential data." *Database*, Volume 2014, doi: 10.1093/database/bau093.

**Book Chapters**

**1**. J. Black, "Cryptography." Invited article for the Encyclopedia of Life Support Systems under the auspices of UNESCO. See `http://www.eolss.net`. 14 pages, March, 2004.

**2**. J. Black, "Authenticated Encryption." Invited article for the *Encyclopedia of Cryptography and Security*, Springer-Verlag. 12 pages. August, 2005.

**Conference Publications (Refereed)**

**1**. J. Black, C. Martel, and H. Qi, "Graph and Hashing Algorithms for Modern Architectures: Design and Performance." *Workshop on Algorithm Engineering — WAE '98*, Saarbrücken, Germany. Second Workshop on Algorithm Engineering, proceedings, pp. 37–48. Full version of this paper available at `theory.cs.ucdavis.edu`.

**2**. J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway, "UMAC: Fast and Secure Message Authentication." *Advances in Cryptology — CRYPTO '99*, Lecture Notes in Computer Science, Vol. 1666, Springer-Verlag, pp. 216–233, 1999. Full version and updated version of this paper available at `www.cs.ucdavis.edu/~rogaway/umac`.

**3**. J. Black and P. Rogaway, "CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions." *Advances in Cryptology — CRYPTO 2000*, Lecture Notes in Computer Science, Vol. 1880, Springer-Verlag, pp. 197–215, 2000.

**4**. P. Rogaway, M. Bellare, J. Black and T. Krovetz, "OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption." *Eighth ACM Conference on Computer and Communications Security (CCS-8)*, ACM Press, pp. 196–205, 2001.

**5**. J. Black and P. Rogaway, "Enciphering Finite Sets of Arbitrary Size." *RSA Data Security Conference, Cryptographer's Track (RSA-CT)*, Lecture Notes in Computer Science, Vol. 2271, Springer-Verlag, pp. 114–130, 2002.

**6**. J. Black and P. Rogaway, "A Block-Cipher Mode of Operation for Parallelizable Message Authentication." *Advances in Cryptology — EUROCRYPT 2002*, Lecture Notes in Computer Science, Vol. 2332, Springer-Verlag, pp. 384–397, 2002.

**7**. J. Black and H. Urtubia, "Side-Channel Attacks on Symmetric Encryption Schemes: The Case for Authenticated Encryption." *USENIX Security Symposium — Security '02*. 10 pages, 2002.

**8**. J. Black, P. Rogaway, and T. Shrimpton, "Black-Box Analysis of the Block-Cipher-Based Hash-Function Constructions from PGV." *Advances in Cryptology — CRYPTO 2002*, Lecture Notes in Computer Science, Vol. 2442. 16 pages, 2002.

**9**. J. Black, P. Rogaway, and T. Shrimpton, "Encryption Scheme Security in the Presence of Key-Dependent Messages." *Selected Areas in Cryptography — SAC 2002*, Lecture Notes in Computer Science, Vol. 2595, 14 pages, 2002.

**10**. R. Motwani, J. Breidenbach and J. Black, "Collocated Dataglyphs for Large Message Storage and Retrieval." *Security, Steganography, and Watermarking of Multimedia Contents VI*, Society for Imaging Science and Technology (I&ST) jointly with International Society for Optical Engineering (SPIE), Vol. 5306, 19 pages, 2004.

**11**. J. Black, M. Cochran and T. Shrimpton, "On the Impossibility of Highly-Efficient Blockcipher-Based Hash Functions." *Advances in Cryptology — EUROCRYPT 2005*, Lecture Notes in Computer Science, Vol. 3494, Springer-Verlag, pp. 526–541, 2005.

**12**. J. Black, M. Cochran and R. Gardner, "Lessons Learned: A Security Analysis of the Internet Chess Club.", *Annual Computer Security Applications Conference — ACSAC 2005*, Tucson AZ, USA, pp. 220–228, 2005.

**13**. J. Black and M. Cochran and T. Highland, "A Study of the MD5 Attacks: Insights and Improvements", *Fast Software Encryption — FSE 2006*, Lecture Notes in Computer Science, Vol. 4047, Springer-Verlag, pp. 262–277, 2006.

**Conference Publications (cont.)**

**14**. J. Black, "The Ideal-Cipher Model, Revisited: An Uninstantiable Blockcipher-Based Hash Function.", *Fast Software Encryption — FSE 2006*, Lecture Notes in Computer Science, Vol. 4047, Springer-Verlag, pp. 328–340, 2006.

**15**. J. Black, "Compare-by-Hash: A Reasoned Analysis", *USENIX Annual Technical Conference — USENIX 2006*, 8 pages, 2006.

**16**. J. Black and M. Cochran, "MAC Reforgeability", *Fast Software Encryption — FSE 2009*, Lecture Notes in Computer Science, Vol. 5665, Springer-Verlag, pp. 345–362, 2009.

**17**. J.H. Huang, J. Black, and S. Mishra, "Security and Privacy in a Sensor-Based Search and Rescue System," *1st ICST/CREATE-NET International Conference on Ad Hoc Networks — ADHOCNETS 2009*, Vol. 28, Springer.

**18**. A. Sayler, D. Grunwald, J. Black, E. White, M. Monaco, "Supporting CS education via virtualization and packages: tools for successfully accommodating "bring-your-own-device" at scale," *SIGCSE 2014*, pp. 313-318, 2014.

**Workshop Publications (Non-Refereed)**

**1**. J. Black and P. Rogaway, "A Suggestion for Handling Arbitrary-Length Messages with the CBC MAC." *NIST Symmetric Key Block Cipher Modes of Operation Workshop—2000*, 4 pages, Sep 2000.

**2**. J. Black and P. Rogaway, "OCB: Proposal to NIST." *2nd NIST Symmetric Key Block Cipher Modes of Operation Workshop—2001*, 36 pages, Aug 2001.

**3**. J. Black and P. Rogaway, "PMAC: Proposal to NIST." *2nd NIST Symmetric Key Block Cipher Modes of Operation Workshop—2001*, 27 pages, Aug 2001.

**Selected Talks**

**1**. Data Structures for Fast Graph Algorithms. Presented at the 1997 UC Davis Workshop on Computing, Davis, USA, October 1997. (See Conference Publication #1.)

**2**. UMAC: Fast and Secure Message Authentication. Presented at CRYPTO '99, Santa Barbara, USA, August 1999. (See Conference Publication #2)

**3**. CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions. Presented at CRYPTO 2000, Santa Barbara, USA, August 2000. (See Conference Publication #3)

**4**. A Suggestion for Handling Arbitrary-Length Messages with the CBC MAC. Presented at NIST Symmetric Key Block Cipher Modes of Operation Workshop—2000, October, 2000; also presented at the 2nd NIST Modes Workshop in Santa Barbara, USA, August 2001.

**5**. Enciphering Finite Sets of Arbitrary Size. Presented at RSA-CT '02, San Jose, USA, February 2002. (See Conference Publication #5)

**6**. A Block-Cipher Mode of Operation for Parallelizable Message Authentication. Presented at EUROCRYPT 2002, Amsterdam, The Netherlands, May 2002. (See Conference Publication #6)

**7**. Side-Channel Attacks on Symmetric Encryption Schemes. Presented at USENIX Security 2002, San Francisco, USA, August 2002. (See Conference Publication #7)

**8**. Practical Cryptography and Autonomic Web Computing. Invited talk at the 47th meeting of the IFIP Working Group 10.4. Rincon, Puerto Rico, January 2005.

**9**. On the Impossibility of Highly-Efficient Blockcipher-Based Hash Functions. Presented at EUROCRYPT 2005, Aarhus, Denmark, May 2005. (See Conference Publication #11)

**10**. The Ideal-Cipher Model, Revisited: An Uninstantiable Blockcipher-Based Hash Function. Presented at FSE 2006, Graz, Austria, March 2006. (See Conference Publication #14)

**11**. Compare-by-Hash: A Reasoned Analysis. Presented at USENIX Technical Conference 2007, Boston, MA, June 2006. (See Conference Publication #15)

**Patents**

**1**. T. McSheery, J. Black, S. Nollet, J. Johnson, and V. Jivan. Distributed-Processing Motion Tracking System for Tracking Individually Modulated Light Points. US Patent 6,324,296 B1. November 2001.

**Funding**

**1**. NCIIA E-Team Grant. "Entrepreneurship for Undergraduates." PI: John Black. Period: 2000-2001. Amount: $6,000.

**2**. University of Nevada Junior Faculty Research Grant. "Fast, Provably-Secure Cryptography." PI: John Black. Period: 2001-2002. Amount: $10,000.

**3**. NSF CAREER Award. "Highly-Optimized Provably-Secure Cryptography." PI: John Black. Period: 2002-2007. Amount: $469,925.

**4**. NSF NeTS Grant. "NeTS ProWIN: Topology And Routing With Steerable Antennas." PI: Dirk Grunwald. Co-PIs: John Black, Douglas Sicker. Period: 2005–2008. Amount: $745,215.

**5**. NSF Cybertrust Grant. "Cryptography for Constrained Environments." PI: John Black. Period: 2005–2008. Amount: $294,887.

| **Teaching History** | ECS 122A — Design and Analysis of Algorithms (UC Davis). Co-taught once with Professor Rogaway; subsequently taught the course independently. |
|---|---|

ECS 122A — Design and Analysis of Algorithms (UC Davis). Co-taught once with Professor Rogaway; subsequently taught the course independently.

CMPSC 290G — Intro to Cryptoanalysis (UCSB).

CS 365 — Discrete Mathematics (UNR).

CS 425 — Software Engineering (UNR).

CS 426 — Senior Projects (UNR). Supervised 11 group projects in topics ranging from fingerprint recognition to audio editing to GUI design.

CS 432 — Computer Networks (UNR). Introduction to low-level networking concepts with an emphasis on network security.

CS 665 — Graduate Analysis of Algorithms (UNR). A typical algorithms course with emphasis on complexity theory.

CS 709 — Modern Cryptography (UNR). A graduate course introducing cryptography and visiting some of the research front.

CS 791G — Computer Network Security (UNR). A seminar course covering various topics related to network security.

CSCI 2270 — Data Structures (CU); Program design, Object orientation, Java, Linked lists, Arrays, Stacks and Queues, Hash tables, Trees, Balanced Binary Trees, Multi-core programming.

CSCI 3104 — Algorithms (CU); Divide-and-conquer, Greedy, Graph Algorithms, NP-Completeness, Quantum Algorithms.

CSCI 3753 — Operating Systems (CU); Scheduling, Virtual Memory, Filesystems, Multi-core systems, Pthreads, Kernel data structures, virtualization, Security.

CSCI 4830 — Network Security (CU); a new course developed to introduce basics of cryptography and network security. Covers SSL, PKI, DDOS attacks, wireless security, buffer overruns, and more.

CSCI 4900 — Solving Puzzles with Computers (CU); a one-unit undergraduate course describing some hard combinatorial puzzles and how computers can be used to attack them.

CSCI 6268 — Foundations of Computer and Network Security (CU); an introductory course covering basic cryptography, cryptographic protocols, attacks, and principles.

CSCI 7000 — Cryptography Seminar (CU); A graduate course introducing basic cryptographic definitions and then making some forays to the research front.

CSCI 7000 — Cryptanalysis Seminar (CU); A graduate course introducing students to cryptanalysis. Differential and linear cryptanalysis, square attack, RSA basics, factoring, protocol errors, lattices, Coppersmith's algorithm.

CSCI 7000 — Quantum Computing (CU): Introduction to quantum circuits, number theory, Shor's Algorithm, Grover's Algorithm.

CSCI 7000 — Ethical Hacking (CU): Network security, nmap, netcat, Kali Linux, Buffer overruns, Format string vulnerabilities, Race Conditions, Web Security, SQL Injections, XSS, CSRF, Wireless.

**Graduate Students**

Rakhi Motwani, M.S., Completed: Spring 2002.

Scott Fritzinger, M.S., Completed: Summer 2002.

Hector Urtubia, M.S., Completed: Spring 2003.

Hiba Fayoumi, M.S., Completed: Summer 2004.

Mary Hedges, M.S., Completed: Spring 2007.

Joesph Dunn, Ph.D., co-advisor with John Bennett, Completed: Summer 2007.

Martin Cochran, Ph.D., Completed: Spring 2008.

Jared Nishikawa, Ph.D., Completed: Spring 2016.

**Undergraduate Students**     Troy Trimble, University of California at San Diego. REU Student, Summer 2003.
Gagan Sekhon, California State University at Hayward. REU Student, Summer 2003.
Ryan Gardner, University of Colorado at Boulder. REU Student, Summer 2004.
Trevor Highland, University of Texas at Austin. REU Student, Summer 2005.

**External Service**

Secretary, International Association for Cryptologic Research, 2005–2007.
Program Committee, ACNS 2015.
Program Committee, CT-RSA 2015.
Program Committee, FSE 2014.
Program Committee, CT-RSA 2014.
Program Committee, CT-RSA 2013.
Program Committee, Eurocrypt 2012.
Program Committee, FSE 2011.
Program Committee, PKC 2011.
Program Committee, CANS 2010.
General Chair, CRYPTO 2009.
Program Committee, CRYPTO 2008.
Program Committee, ACNS 2008.
Program Committee, RSA-CT 2007.
Program Committee, ISC 2007.
Program Committee, ACNS 2007.
Program Committee, ACM CCS 2006.
Program Committee, CANS 2006.
Program Committee, ICISC 2006.
Program Committee, SECRYPT 2006.
Program Committee, ACSAC 2006.
Program Committee, CRYPTO 2005.
Program Committee, SAC 2005.
Program Committee, ICISC 2005.
Program Committee, CANS 2005.
Program Committee, IEEE SISW 2005.
Program Committee, CRYPTO 2004.
Program Committee, EUROCRYPT 2004.
Program Committee, RSA-CT 2003.
NSF CISE Panelist, 2001, 2003, 2005, 2006, 2007, 2009.
Referee for Journal of Cryptography, 1999-2006.
Referee for Software: Practice and Experience, 2005.
Referee for IEEE Communications Magazine, 2005.
Referee for IEEE Transactions on Circuits and Systems I, 2005.
Referee for IEEE Computer, 2005.
Referee for Journal of Computer Security, 2004.
Referee for IEEE Transactions on Information Theory, 2003.
Referee for IEEE Transactions on Computers, 2002.
Reviewer for CRYPTO 1999–2002, SODA 1998, SPAA 2002, Asiacrypt 2004, EURO-CRYPT 2006.

Developed `CryptoStats` web site: an application which tracks publication rates by year, by author, by conference in the two main cryptography conferences. It was heavily used in my community (on average 240 hits per month), 2003-2009.

ACM Programming Contest problem composer, 2003–2007.
ACM Programming Contest site administrator, 2005.

Graduate Student Mixer organizer, CRYPTO 2005.

**Internal Service**     Chair, Computing Committee, 2010–2011, 2012–2015.

Chair, Space Committee, 2012–2015.

Liaison, Casey Feldman Foundation, 2010–2015.

Member, Departmental Executive Committee, 2003–2005, 2007–2009, 2013-2015.

Member, Executive Committee, Computer and Communications Security Center, 2003–2006.

Member, Departmental Search Committee, 2003–2006, 2012–2014.

Chair, Departmental Search Committee, 2008–2009.

Member, Graduate Committee, 2005–2006.

Developed departmental voting software, now used for all departmental votes and college votes.