

**Department of Computer Science, The George Washington University**  
**Colloquium**



**Professor Ronald L. Rivest**  
**Viterbi Professor of Computer Science**  
**Massachusetts Institute of Technology**

Professor Rivest is the Viterbi Professor of Computer Science in MIT's Department of Electrical Engineering and Computer Science. He is a member of MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL), a member of the lab's Theory of Computation Group and is a leader of its Cryptography and Information Security Group.

Professor Rivest is a co-inventor of the RSA public-key cryptosystem. He has served as a Director of the International Association for Cryptologic Research, the organizing body for the Eurocrypt and Crypto conferences, and as a Director of the Financial Cryptography Association. He is also a founder of RSA Data Security and of Verisign.

Professor Rivest is a member of the National Academy of Engineering and of the National Academy of Sciences, and is a Fellow of the Association for Computing Machinery, the International Association for Cryptographic Research, and the American Academy of Arts and Sciences. He is also on the Advisory Board for the Electronic Privacy Information Center.

Professor Rivest has won numerous awards. Together with Adi Shamir and Len Adleman, he has been awarded the 2000 IEEE Koji Kobayashi Computers and Communications Award and the Secure Computing Lifetime Achievement Award. He is a recipient of the Marconi Award, and has also received, together with Shamir and Adleman, the 2002 ACM Turing Award and the 2009 NEC C&C Award.

Most recently, Professor Rivest has served on the U.S. Technical Guidelines Development Committee, which has drafted proposed standards for certifying voting system in the U.S.

**Department of Computer Science, The George Washington University**  
**Colloquium**

**Professor Ronald L. Rivest**  
**Viterbi Professor of Computer Science**  
**Massachusetts Institute of Technology**

Room 308/Parks Room, Marvin Center, 800 21st NW, George Washington University  
Date: November 9, 2009  
Time: 5pm

**Security of Voting Systems**

While running an election sounds simple, it is in fact extremely challenging. Not only are there millions of voters to be authenticated and millions of votes to be carefully collected, counted, and stored, there are now millions of "voting machines" containing millions of lines of code to be evaluated for security vulnerabilities. Moreover, voting systems have a unique requirement: the voter must not be given a "receipt" that would allow them to prove how they voted to someone else---otherwise the voter could be coerced or bribed into voting a certain way. This lack of receipts makes the design of secure voting system much more challenging than, say, the security of banking systems (where receipts are the norm).

We discuss some of the recent trends and innovations in voting systems, as well as some of the new requirements being placed upon voting systems in the U.S., and describe some promising directions for resolving the conflicts inherent in voting system requirements, including some approaches based on cryptography. We also describe the use of the "Scantegrity II" end-to-end voting system, developed by David Chaum and researchers from MIT, GW, UMBC, Ottawa, and Waterloo, in last Tuesday's election in the city of Takoma Park, Maryland.