Guest Editorial
Special Issue on Electronic Voting

I. Background

THIS special issue provides representative samples of the excellent research being carried out in electronic voting today—in areas as diverse as statistics, usability, cryptography, formal methods in security and experimental computer security analysis. It is perhaps the first broadly defined special issue of a technical journal in this rapidly growing and important research area.

The last few years have witnessed the large-scale deployment of electronic voting systems worldwide: both optical scan voting systems and direct recording electronic (DRE) systems. The latter have drawn the most attention because of the detection, by voting researchers, of a wide variety of flaws that could be used to manipulate election outcomes. At the same time, several new voting systems, that would not have similar flaws, have been proposed, prototyped, and used in binding elections. The possibility of having an impact on deployed systems has transformed the field of voting technology research to one that is now growing rapidly, attracting researchers of various backgrounds. In this multidisciplinary special issue, we bring together several of the most interesting new results in the area.

II. The Papers

We begin the special issue with two papers illustrating two different approaches to improving the integrity of elections that use optical scan equipment.

Antonyan *et al.* describe new audit procedures, and their implementation for elections in the state of Connecticut, U.S., on the request of the Office of the Secretary of the State.

Chaum *et al.* describe Scantegrity II, which will be used by Takoma Park, MD, for its municipal election in November 2009. The paper describes the use of confirmation codes for cryptographic audits of the election outcome, which can be performed by voters and election observers, and are not restricted to privileged individuals.

Fink, Sherman, and Carback describe the use of trusted platform modules (TPMs) to reduce the trusted computing base of DREs. This approach enables the early detection of threats to election integrity.

Gardner, Garera, and Rubin present a new approach by which a human, such as a poll worker, can determine whether the software on an electronic voting machine has been modified, using the time taken by the computer to respond to a challenge issued by the human. If the software is changed, differences in main and cache memory access times, or CPU clock cycle times, cause the response times to be greater.

Villafiorita, Weldemariam, and Tiella describe ProVotE, an electronic voting system with a voter-verified paper audit trail (VVPAT) which has been used for trials and elections in Italy. They describe the design of the user interface, the use of formal approaches for the validation of the main parts of the system, and the rigorous analysis of important procedures.

The paper on the *Prêt à Voter* system, by Ryan *et al.*, presents a unified description of various versions of one of the earliest voting systems where voters do not need access to an electronic system to cast their votes, yet can be assured of verifiability and privacy.

Van de Graaf proposes a simple voting protocol that provides unconditional privacy, merging the ballot design of *Prêt à Voter* with unconditionally hiding commitments in the ballot processing aspects of the Punchscan voting protocol.

Benaloh *et al.* present a method for the efficient, universally verifiable, and coercion-resistant tallying of votes in single transferable vote elections. These types of elections, where voters rank candidates, pose unique challenges that remain among the most difficult to address.

Henry, Stinson, and Sui present a rigorous approach to determining the effectiveness of attacks, on the ThreeBallot voting system, that are based on the voter's receipt and the bulletin board.

Stark describes a method to determine whether to hand count an entire paper audit trail for an election. This method counts randomly chosen samples of ballot batches in stages, using an upper bound on the P-value of the hypothesis that the election outcome is incorrect to determine whether to proceed to the next stage or to stop the audit.

Campbell and Byrne address the important issue of ballot presentation and its impact on the voter experience. Their paper describes the results of surveys performed to determine whether straight-party voting (where voters may cast votes for a single party, in many races, with one action) causes voter confusion.

Schryen and Rich examine three large-scale government elections held on the Internet, in Estonia, the Netherlands, and Switzerland, to understand their use of security technology and procedures. The paper finds that early adopters have neglected to address several security threats.

The final paper—by Bohli *et al.*—describes the use of an existing approach, Bingo Voting, to improve the integrity and coercion-resistance of voting systems.

We hope you enjoy the articles in this special issue, and that it attracts new researchers to electronic voting from the many communities that read the IEEE Transactions on Information Forensics and Security.

Ronald L. Rivest, *Lead Guest Editor*
Massachusetts Institute of Technology
Cambridge, MA 02139 USA

Digital Object Identifier 10.1109/TIFS.2009.2034721

DAVID CHAUM, *Guest Editor*
Voting Systems Institute
Los Angeles, CA 90064 USA

BART PRENEEL, *Guest Editor*
Katholieke Universiteit Leuven
Leuven, B-3001 Belgium

AVIEL D. RUBIN, *Guest Editor*
Johns Hopkins University
Baltimore, MD 21218 USA

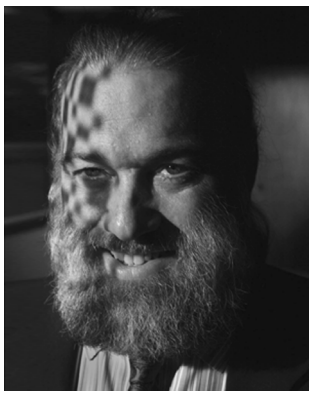
DONALD G. SAARI, *Guest Editor*
University of California
Irvine, CA 92697-5100 USA

POORVI L. VORA, *Guest Editor*
The George Washington University
Washington, DC 20052 USA

Ronald L. Rivest received the B.A. degree in mathematics from Yale University in 1969, and the Ph.D. degree in computer science from Stanford University in 1974.

He is the Viterbi Professor of Computer Science in the Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology (MIT). 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. His research interests are in cryptography, computer and network security, algorithms, and voting systems. He is an inventor of the RSA public-key cryptosystem, and has extensive experience in cryptographic design and cryptanalysis. He is a founder of RSA Data Security and a cofounder of Verisign and of Peppercoin.

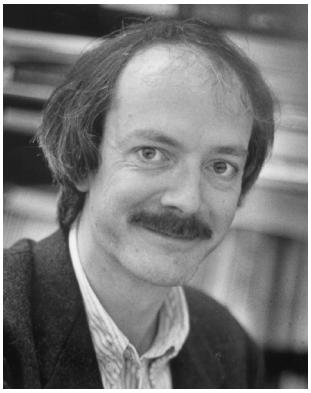
Prof. Rivest is a member of the National Academy of Engineering, the National Academy of Sciences, and is a Fellow of the Association for Computing Machinery, the International Association for Cryptographic Research, and the American Academy of Arts and Sciences. He also serves on the EPIC Advisory Board. Together with Prof. Adi Shamir and Prof. Len Adleman, he has been awarded the 2002 ACM Turing Award. He has received an honorary degree (the "laurea honoris causa") from the University of Rome. In 2005, he received the MITX Lifetime Achievement Award; in 2007, he received both the Computers, Freedom and Privacy Conference "Distinguished Innovator" award, and the Marconi Prize. He has served as a Director of the International Association for Cryptologic Research, and of the Financial Cryptography Association. Most recently, he has served on the Technical Guidelines Development Committee, an advisory board to the U.S. Election Assistance Commission.



David Chaum received the M.S. degree and the Ph.D. degree in computer science from the University of California, Berkeley, in 1980 and 1983, respectively.

He founded DigiCash, Inc., where he was CEO from 1993 to 1998. Before that, he built and lead the Cryptography Group at Centrum voor Wiskunde en Informatica (Center for Mathematics and Computer Science), Amsterdam, The Netherlands, from 1985 to 1992. He has also held positions at University of California Santa Barbara and at New York University Graduate School of Business. He has published over 45 original technical articles and received over 17 U.S. patents. He is widely considered to have invented secure electronic voting, with a paper describing a technique for anonymous electronic voting in 1981, and several papers since. He is also generally associated with the invention of electronic money and anonymous credentials. He was the first to propose: mix networks, dining-cryptographer networks, blind signatures, untraceable credentials, minimum disclosure, group and undeniable signatures. He has also made early and fundamental contributions to the area of multiparty computations.

Dr. Chaum is founder of the International Association for Cryptographic Research (IACR) and cofounder of Workshop on Trustworthy Elections (WOTE), a series of conferences and its sponsoring organization the International Association for Voting Systems Sciences (IAVOSS).



Bart Preneel received the Master's degree in electrical engineering and the Doctorate in applied sciences (cryptology) from the Katholieke Universiteit Leuven, Belgium, in 1987 and 1993, respectively.

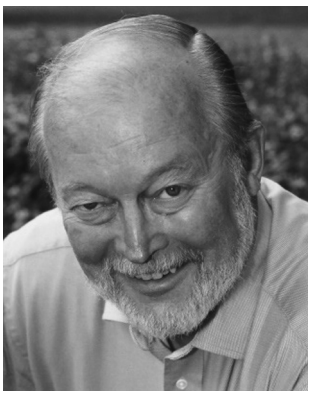
He is currently full professor at the Katholieke Universiteit Leuven. He has been a visiting professor at five universities in Europe and a research fellow at the University of California at Berkeley. He has authored and coauthored more than 300 reviewed scientific publications and is inventor of three patents. His main research interests are cryptography and information security.

Prof. Preneel is president of the International Association for Cryptologic Research (IACR) and of Leuven Security Excellence Consortium (L-SEC vzw.), an association of 60 companies and research institutions in the area of e-security. He is a member of the Editorial Board of the *Journal of Cryptology*, the IEEE TRANSACTIONS ON FORENSICS AND INFORMATION SECURITY, and the *International Journal of Information and Computer Security*. He has participated in more than 20 research projects sponsored by the European Commission, for five of these as project manager. He has been program chair of 12 international conferences (including Eurocrypt 2000, SAC 2005, and ISC 2006) and invited speaker at more than 50 conferences. In 2003, he received the European Information Security Award in the area of academic research, and he received an honorary Certified Information Security Manager (CISM) designation by the Information Systems Audit and Control Association (ISACA).

Aviel D. Rubin received the B.S., M.S.E., and Ph.D. degrees from the University of Michigan, in 1989, 1991, and 1994, respectively.

He is Professor of Computer Science and Technical Director of the Information Security Institute, Johns Hopkins University. He directs the NSF-funded ACCURATE Center for Correct, Usable, Reliable, Auditable and Transparent Elections. Prior to joining Johns Hopkins, he was a Research Scientist at AT&T Laboratories. He is also a cofounder of Independent Security Evaluators (securityevaluators.com), a security consulting firm. He has testified before the U.S. House and Senate on multiple occasions, and he is author of several books including *Brave New Ballot* (Random House, 2006), *Firewalls and Internet Security*, second edition (with Bill Cheswick and Steve Bellovin, Addison Wesley, 2003), *White-Hat Security Arsenal* (Addison Wesley, 2001), and *Web Security Sourcebook* (with Dan Geer and Marcus Ranum, Wiley, 1997). He is Associate Editor of IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, Associate Editor of *IEEE Security and Privacy*, and an Advisory Board member of Springer's Information Security and Cryptography Book Series.

In January 2004, *Baltimore Magazine* named Dr. Rubin a Baltimorean of the Year for his work in safeguarding the integrity of our election process, and he is also the recipient of the 2004 Electronic Frontiers Foundation Pioneer Award.



Donald G. Saari received the B.S. degree in mathematics from Michigan Technological University in 1962, and the M.S. and Ph.D. degrees in mathematics from Purdue University in 1964 and 1967, respectively. His post-doc position was in the Yale Astronomy Department.

He is Distinguished Professor of Mathematics and Economics, and Director of the Institute for Mathematical Behavioral Sciences, at the University of California, Irvine. He served on the Mathematics faculty at Northwestern University, where he was the Arthur and Gladys Pancoe Professor of Mathematics. He has published over 175 refereed articles and written or edited eleven books, including: *Chaotic Elections! A Mathematician Looks at Voting* (American Math Society, 2001), *Basic Geometry of Voting* (Springer-Verlag, 1995), and *Disposing Dictators; Demystifying Voting Paradoxes* (Cambridge University Press, 2008).

Prof. Saari is a member of the National Academy of Sciences, a member of the Finnish Academy of Science and Letters, a Fellow of the American Academy of Arts and Sciences, a Fellow of the American Association for the Advancement of Science, and a Fellow of SIAM. He has been awarded honorary doctoral degrees by Michigan Technological University, Université de Caen, (Caen, France), Purdue University, and the University of Turku (Turku, Finland). He received the Allendoerfer Award, the Chauvenet Prize and the Lester R. Ford Award of the Mathematical Association of America, and the Duncan Black Research Award of the Public Choice Society.

Poorvi L. Vora received the B.Tech. degree in electrical and electronic engineering from IIT Mumbai, in 1986, the M.S. and Ph.D. degrees in electrical engineering from North Carolina State University (NCSU), in 1988 and 1993, and the M.S. in mathematics from Cornell University, in 1990.

She is an Associate Professor in the Department of Computer Science at The George Washington University, Washington, D.C., where she has been on the faculty since 2003. Before 2003, she worked at Hewlett-Packard (HP) Company in various positions in HP Laboratories, as well as in the Imaging and Printing Group (IPG). Her current research interests are in the application of ideas from communication theory and signal processing to problems in security, such as electronic voting, cryptology, and counterfeit deterrence.