Secret Ballot Receipts

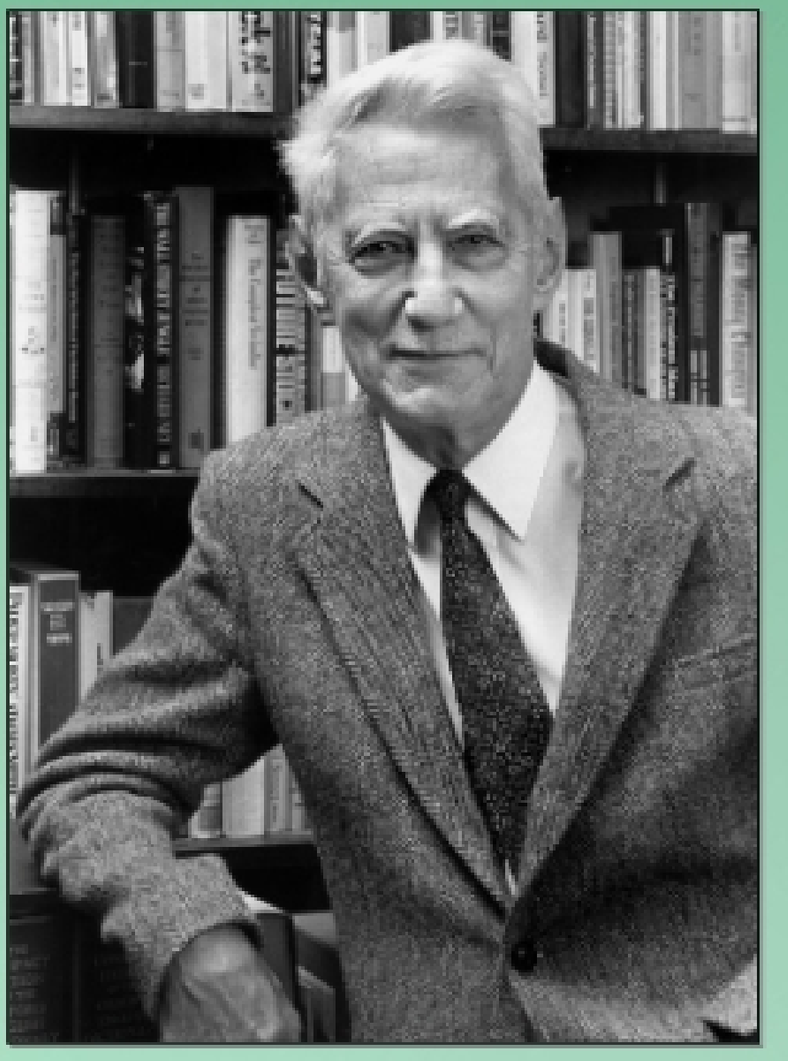
True Voter-Verifiable Elections

Richard Carback
Kevin Fisher
Sandi Lwin

CMSC 691v
April 3, 2005

References

1. M. Naor and A. Shamir, "Visual Cryptography," *Proc. Advances in Cryptology (Eurocrypt 94)*, A. De Santis, ed., LNCS 950, Springer-Verlag, 1995, pp. 1–12.
2. C.E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical J.*, no. 28, 1949, pp. 656–715.



PURPOSE The IEEE Computer Society is the world's largest association of computing professionals, and is the leading provider of technical information in the field.

MEMBERSHIP Members receive the monthly magazine COMPUTER, discounts, and opportunities to serve (all activities are led by volunteer members). Membership is open to all IEEE members, affiliate society members, and others interested in the computer field.

COMPUTER SOCIETY WEB SITE The IEEE Computer Society's Web site, at **www.computer.org**, offers information and samples from the society's publications and conferences, as well as a broad range of information about technical committees, standards, student activities, and more.

BOARD OF GOVERNORS
Term Expiring 2004: *Jean M. Bacon, Ricardo Baeza-Yates, Deborah M. Cooper, George V. Cybenko, Haruhisha Ichikawa, Thomas W. Williams, Yervant Zorian*
Term Expiring 2005: *Oscar N. Garcia, Mark A. Grant, Michel Israel, Stephen B. Seidman, Kathleen M. Swigger, Makoto Takizawa, Michael R. Williams*
Term Expiring 2006: *Mark Christensen, Alan Clements, Annie Combelles, Ann Gates, Susan Mengel, James W. Moore, Bill Schilit*
Next Board Meeting: *20 Feb. 2004, Savannah, GA*

IEEE OFFICERS
President: ARTHUR W. WINSTON
President-Elect: W. CLEON ANDERSON
Past President: MICHAEL S. ADLER
Executive Director: DANIEL J. SENESE
Secretary: MOHAMED EL-HAWARY
Treasurer: PEDRO A. RAY
VP, Educational Activities: JAMES M. TIEN
VP, Publication Services & Products: MICHAEL R. LIGHTNER
VP, Regional Activities: MARC T. APTER
VP, Standards Association: JAMES T. CARLO
VP, Technical Activities: RALPH W. WYNDRUM JR.
IEEE Division V Director: GENE H. HOFFNAGLE
IEEE Division VIII Director: JAMES D. ISAAK
President, 2003–04: JOHN W. STEADMAN

IEEE COMPUTER SOCIETY

COMPUTER SOCIETY OFFICES
Headquarters Office
1730 Massachusetts Ave. NW
Washington, DC 20036-1992
Phone: +1 202 371 0101
Fax: +1 202 728 9614
E-mail: help@computer.org

Publications Office
10662 Los Vaqueros Cir., PO Box 3014
Los Alamitos, CA 90720-1314
Phone: +1 714 821-8380
E-mail: help@computer.org
Membership and Publication Orders:
Phone: +1 800 272 6657
Fax: +1 714 821 4641
E-mail: help@computer.org

Asia/Pacific Office
Watanabe Building
1-4-2 Minami-Aoyama, Minato-ku
Tokyo 107-0062, Japan
Phone: +81 3 3408 3118
Fax: +81 3 3408 3553
E-mail: tokyo.ofc@computer.org

IEEE

EXECUTIVE COMMITTEE
President:
CARL K. CHANG*
Computer Science Dept.
Iowa State University
Ames, IA 50011-1040
Phone: +1 515 294 0377
Fax: +1 515 294 0258
c.chang@computer.org
President-Elect: GERALD L. ENGEL*
Past President: STEPHEN L. DIAMOND*
VP, Educational Activities: MURALI VARANASI*
VP, Electronic Products and Services:
LOWELL G. JOHNSON (1ST VP)*
VP, Conferences and Tutorials:
CHRISTINA SCHOBER*
VP, Chapters Activities:
RICHARD A. KEMMERER (2ND VP)†
VP, Publications: MICHAEL R. WILLIAMS†
VP, Standards Activities: JAMES W. MOORE†
VP, Technical Activities: YERVANT ZORIAN†
Secretary: OSCAR N. GARCIA*
Treasurer: RANGACHAR KASTURI†
2003–2004 IEEE Division V Director:
GENE H. HOFFNAGLE†
2003–2004 IEEE Division VIII Director:
JAMES D. ISAAK†
2004 IEEE Division VIII Director-Elect:
STEPHEN L. DIAMOND*
Computer Editor in Chief: DORIS L. CARVER†
Executive Director: DAVID W. HENNAGE†
* voting member of the Board of Governors
† nonvoting member of the Board of Governors

EXECUTIVE STAFF
Executive Director: DAVID W. HENNAGE
Assoc. Executive Director: ANNE MARIE KELLY
Publisher: ANGELA BURGESS
Assistant Publisher: DICK PRICE
Director, Finance & Administration:
VIOLET S. DOAN
Director, Information Technology & Services:
ROBERT CARE
Manager, Research & Planning: JOHN C. KEATON

Introduction

System Features

- Magic receipt
  - Vote visible in voting booth
  - Vote invisible, verifiable outside voting booth
- Trusted voting machines unnecessary
- Provisional ballots are ballots, too
- Vote from anywhere
- ~~Adjudicate today's ballots~~ Delegate tomorrow
- ~~Eliminates common indoor allergens~~
  - ~~Even pet dander~~!
- ~~Boosts gas mileage up to~~ 13%