

Secret Ballot Receipts

True Voter-Verifiable Elections

Richard Carback
Kevin Fisher
Sandi Lwin

CMSC
691v
April 3,
2005

maries have not been shown to be effective or workable in general and have been replaced in Brazil. This movement does, however, indicate a growing level of public concern, and the two printing approaches could even be combined. The sad truth, however, is that the process of deciding which types of systems to deploy has so far for the most part been closed and informed neither by explicit performance requirements nor generally accepted security practices.

The receipt system presented here offers a new level of integrity, access, robustness, and adjudication, all at lower cost, that make it a compelling way to secure polling-place elections—and it should be the only way acceptable now. □

Acknowledgments

It is a pleasure to acknowledge Rex Rivest, who served as a superb sounding board for ideas. The "WOTE" workshop was also very stimulating. Larry Jis Dalboer and Lori Wikström provided a lot of help. Detailed comments from Josh Bonalok, Paul Capt, David Jefferson, Doug Jones, and Andrea Riva, as well as feedback from Je-

rony Byrnes, Dan Boneh's group, Stuart Haber, Roberto Ryan, Markus Schödl, and Adi Shamir were also helpful.

References

1. M. Naor and A. Shamir, "Visual Cryptography," *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, pp. 656–715.

David Chaum is currently affiliated with several companies, universities, and international projects. Widely recognized as the inventor of electronic cash, he also originated a number of cryptographic techniques, general results, and tools that allow individuals to protect their identity and related data in interactions with organizations. He has many original technical publications and 23 separate cryptographically related patent filings. Chaum has a PhD in computer science from the University of California, Berkeley. He has led a number of crypto research groups, and founded DigiCash and the International Association for Cryptologic Research (IACR). Contact him at info@chaum.com.

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 New facts 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: Juan M. Alonso, Nicolás Becerra-Tasso, Deborah M. Cooper, George V. Cybenko, Elizabeth Eitelberg, Thomas W. Williams, Vincent Zarka

Term Expiring 2005: Carol K. Carnes, Mark A. Green, Michael Green, Stephen H. Heuleman, Kathleen M. Siggitt, Mahesh Takkar, Michael E. Williams

Term Expiring 2006: Mark Christensen, Alan Cline, Anne Corbett, Ann Gains, Susan Morgan, James W. Moore, Neil Schillo

Next Board Meeting: 27 Feb. 2004, Savannah, GA

IEEE OFFICERS

President: ARTHUR W. WINSTON

President-Elect: W. CLEON ANDERSON

Past President: MICHAEL S. ADLER

Executive Director: DANIEL J. SCHNESE

Secretary: MOHAMED EL-HAWARY

Treasurer: PEDRO A. RAY

VP, Educational Activities: JAMES M. TIEN

VP, Public Services/Products: MICHAEL H. LIGHTNER

VP, Regional Activities: MARGY T. APTER

VP, Standards Association: JAMES T. CARLO

VP, Technical Activities: RALPH B. WYNDRUM JR.

2002 Division I Director: GENE H. HOFFNAGLE

2002 Division III Director: JAMES D. ISAAC

President, 2002-05: JOHN W. STEADMAN



COMPUTER SOCIETY OFFICES

Headquarters Office

4700 Massachusetts Ave. NW
Washington, DC 20037-2050
Phone: +1 202 371 0900
Fax: +1 202 739 8624
E-mail: hq@computer.org

Publications Office

2000 The Topanga Cir., PO Box 2014
Arcadia, CA 91709-2114
Phone: +1 714 821-0300
E-mail: pub@computer.org

Membership and Publications Orders

Phone: +1 800 272-6637
Fax: +1 714 821 8517
E-mail: help@computer.org

Asia/Pacific Office

Watanabe Building
2-4-2 Watanabe-Doyama, Minato-ku
Tokyo 107-0962, Japan
Phone: +81 3 3469 3748
Fax: +81 3 3469 3553
E-mail: adpa@computer.org



EXECUTIVE COMMITTEE

President

CARL K. CHANG*

Computer Science Dept.

1000 State University

Alex., VA 22301-1040

Phone: +1 551 291-6377

Fax: +1 551 291-6338

E-mail: chang@computer.org

President-Elect: GERALD L. ENGEL*

Past President: STEPHEN L. DIAMOND*

VP, Educational Activities: MURALI VARMA*

VP, Electronic Products and Services:

LOWELL G. JOHNSON (1ST VP)*

VP, Conferences and Exhibits:

CHRISTINA SCHUBERT*

VP, Chapters Activities:

RICHARD A. KEMMERER (2ND VP)*

VP, Publications: MORRIS R. WILLIAMS*

VP, Standards Activities: JAMES B. MOORE*

VP, Technical Activities: YERWANT ZOFRANI*

Secretary: OSCAR N. GARCIA*

Treasurer: RANDA CHAR KASTURI*

2002-2004 IEEE Division I Director:

GENE H. HOFFNAGLE†

2003-2004 IEEE Division IV Director:

JAMES D. ISAAC†

2004 IEEE Division IV Director-Elect:

STEPHEN L. DIAMOND†

Computer Editor in Chief: PETER 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 MARE KELLY

Publisher: ANGELA BUFOSSO

Assistant Publisher: DIK PRICE

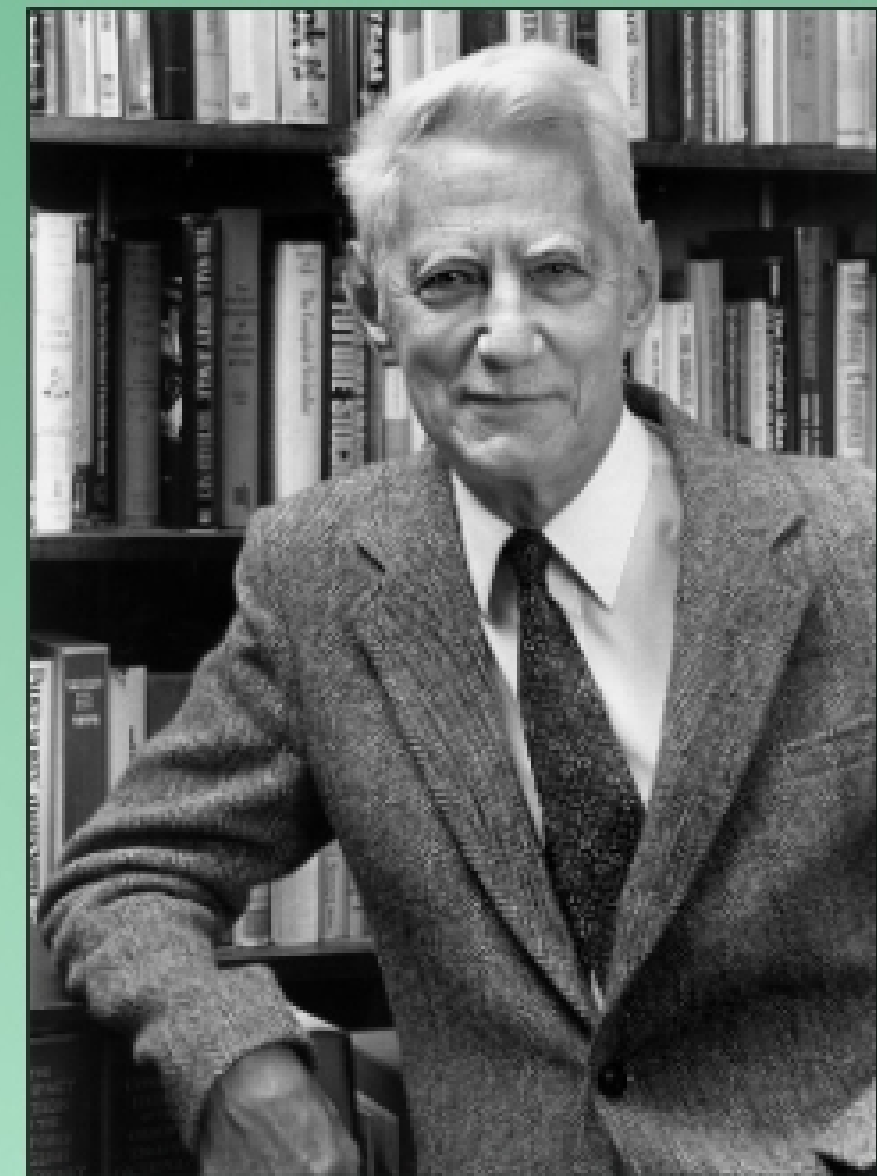
Director, Finance & Admin. Services:

WOLFE S. DODD

Director, Information Technology & Services:

ROBERT DARR

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
- ~~Dejeper, a n d e e s t f a d j u k e p t e~~ tomorrow
- ~~Eliminates common indoor allergens~~
 - ~~Even pet dander!~~
- ~~Boosts gas mileage up to 13%~~