Berner Fachhochschule - Technik und Informatik

e-Voting Protocols

Overview and Comparison

Dr. Rolf Haenni

May 21st, 2008

Outline

Introduction

Outline

Outline

Outline

Cryptographic Basics

Symmetric Encryption	$c = E(m, k)$
Symmetric Decryption	$m = D(c, k)$
Message Digest	$h(m)$
Public/Private Keys	X_e, X_d
Asymmetric Encryption	$c = E(m, X_e)$
Asymmetric Decryption	$m = D(c, X_d)$
Signature	$s = S(m, X_d)$
Verification	$V(m, s, X_e) \in \{yes, not\}$

Blind Signatures

- Blind signatures were proposed by Chaum (1983)
- Based on RSA
- Random number r (relative prime to N)
- Blinding factor: r^{X_e}
- Blinded message: $m \times r^{X_e}$
- Blind signature: $s' = S(m \times r^{X_e}, X_d) = (m \times r^{X_e})^{X_d} = m^{X_d} \times r$
- Unblinded signature: $s = s' \times r^{-1} = m^{X_d} = S(m, X_d)$

  $\Rightarrow$ the message is signed without its content being revealed

Anonymous Channels

- Many voting protocol rely on *anonymous channels* to cast vote ballots
  - → Mix-net approach (Chaum, 1981)
  - → DC-net approach (Chaum, 1988)
  - → Onion routing (Goldschlag, Reed, Syverson, 1999)
- The idea is to establish anonymity (vote privacy) using untraceable or hard-to-trace messages
- Voters use digital pseudonyms to conceal their identities
- An anonymous channel consists of a *chain* of proxy servers (mix agents), which establish the unlinkability between voters and pseudonyms
- If all but one of the proxy servers are compromised by the tracer, untraceability can still be achieved

Homomorphic Encryption

- Form of encryption where one can perform a specific algebraic operation on the plaintext by performing a (possibly different) algebraic operation on the ciphertext (Cramer et al. 1997)
  - → using zero-knowledge
- Encrypted votes can be counted without being decrypted
- If the list of encrypted votes are published, every voter can
  - → verify if his/her vote is on the list
  - → recount the votes
- Only applicable if votes are additive (e.g. yes/no votes)
- Implemented by Lehtonen (2001) and the commercial product VoteHere, but otherwise not very popular in practice

Outline

Classification of Protocols

- Most practical voting protocols use a PKI
  - → most of them use blind signatures
  - → most of them use anonymous channels
- Most protocols use 2 administering servers (some use 1 or 3)
  - → Validator: checks the voter's eligibility, issues the ballot
  - → Tallier: collect, counts, and publishes the votes
- Full trust in both the validator and the tallier is usually not necessary (the ideal case)
- Most protocols are not *receipt-free* (vote buying is possible)
- see Røsland (2004) for a good survey

Early History of Voting Protocols

- Salomaa (1991): Two-agency protocol
  - → no blind signature
- Nurmi, Salomaa, Santean (1991): One-agency protocol
  - → no blind signature
  - → uses ANDOS (all-or-nothing disclosure of secrets)
- Fujioka, Okamoto, Ohta (1992)
  - → blind signature
  - → uses anonymous channels
  - → not receipt-free
  - → predecessor of many other protocols
- FOO92 with slight modifications is generally regarded as the best voting protocol

FOO92-Based Protocols I

- Baraani-Dastjerdi, Pieprzyk, Safavi-Naini (1994)
  - → improvement of FOO92
- Okamoto (1996, 1997)
  - → receipt-free versions of FOO92
- Cranor, Cytron (1997): Sensus
  - → variant of FOO92
  - → implemented and tested at the Washington University
- Herschberg (1997), DuRette (1999): EVOX
  - → implementation of FOO92 (master thesis, bachelor thesis)
  - → MIT campus-wide student elections
- Ohkubo, Miura, Abe, Fujioka, Okamoto (1999)

FOO92-Based Protocols II

→ an improvement of FOO92

- Riera, Borrell (1999)
  - → protocol based on mix-nets and blind signature
  - → implemented in SCYTL (used in Neuchâtel)
- Ray, Ray, Narasimhamurthi (2001)
  - → similar to FOO92 and Sensus
  - → 3 administrating agents (ballot distributor, certifying authority, vote compiler)
  - → no anonymous channel
  - → session may be traced back to an IP address but not to a voter
  - → implemented at BFH-TI, see Aeby and Wiget (2007)
- Kim (2002): Votopia
  - → built for WorldCup 2002 Korea/Japan

FOO92-Based Protocols III

- → used to choose MVP and best goalkeeper
- → based on Ohkubo et al. (1999)

- Kofler, Krimmer, Prosser (2003):
  - → 2-phase variant of FOO92
  - → voter registering is separated from vote casting
- Joaquim, Zuquete, Ferreira (2004): REVS
  - → fault tolerant variant of the EVOX implementation
- Baiardi et al. (2005): SEAS
  - → variant of the Sensus protocol
  - → prototype implementation (Java applet, XML)
- Anane, Freeland, Theodoropoulos (2007)
  - → another prototype implementation of FOO92

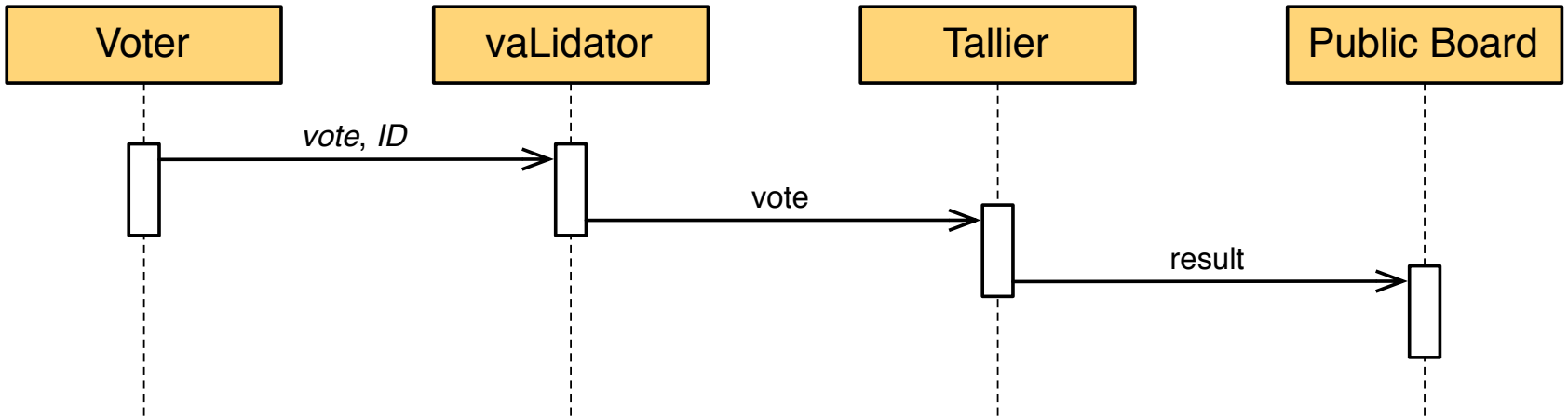
Commercial Systems

Kiayias et al. (2006) survey several voting systems from the commercial world. These proprietary systems do not generally make their implementations publicly or freely available, nor do they appear to offer coercion resistance. The California top-to-bottom review of commercial electronic voting systems suggests that these systems offer completely inadequate security.

$\Rightarrow$ http://www.sos.ca.gov/elections/elections_vsr.htm

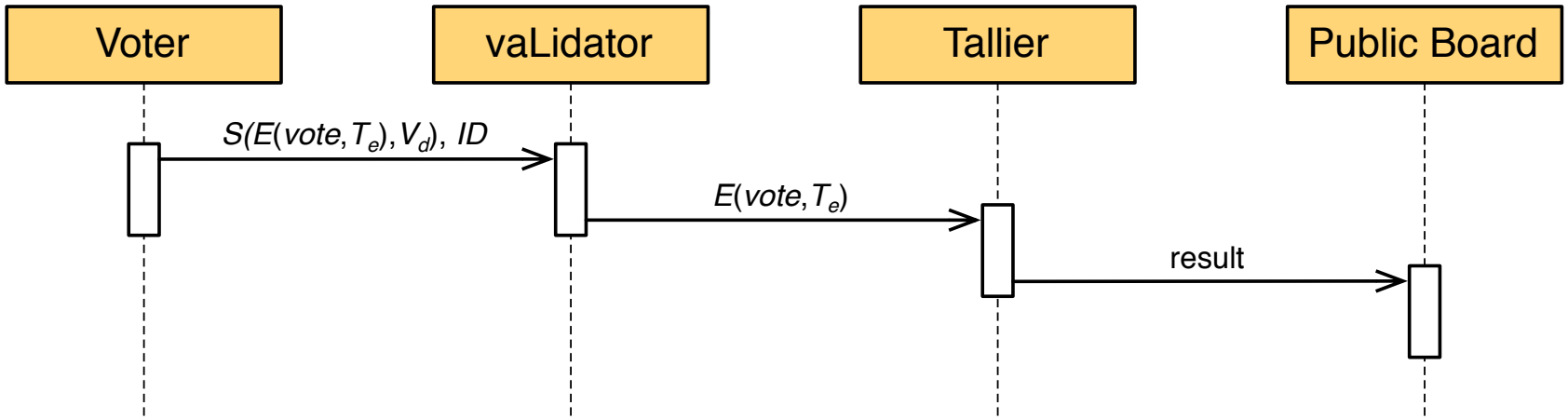
Outline

A Simple (Non-Crypto) Protocol



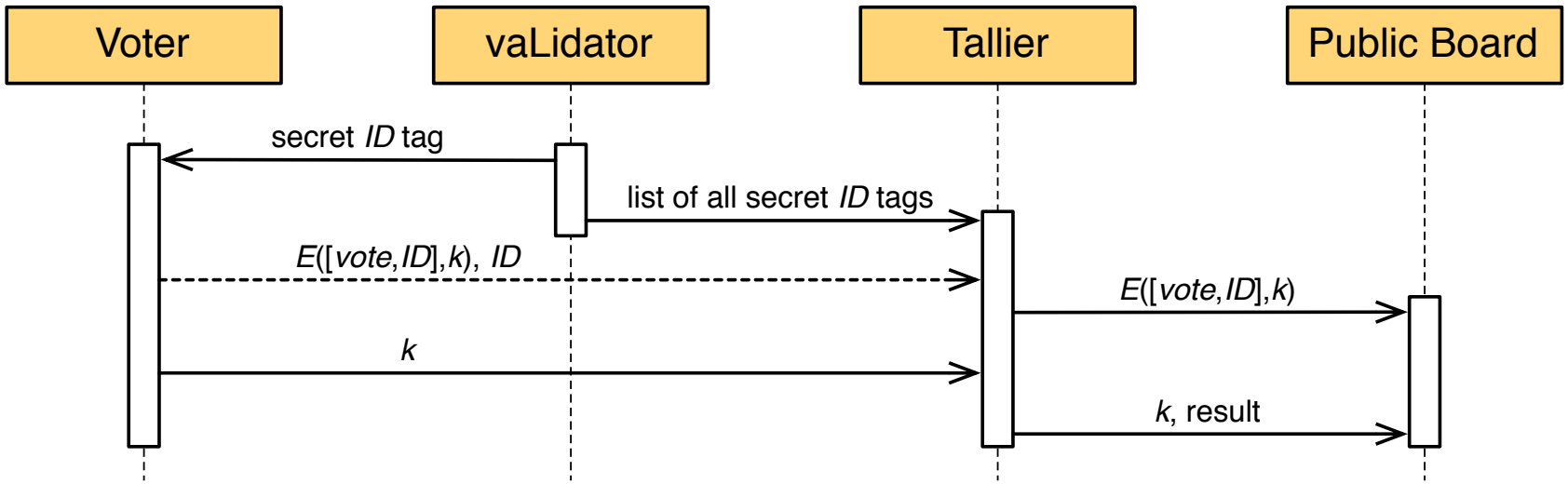
- Good: simple, flexible, mobile
- Bad: inherently insecure

A Simple Cryptographic Protocol



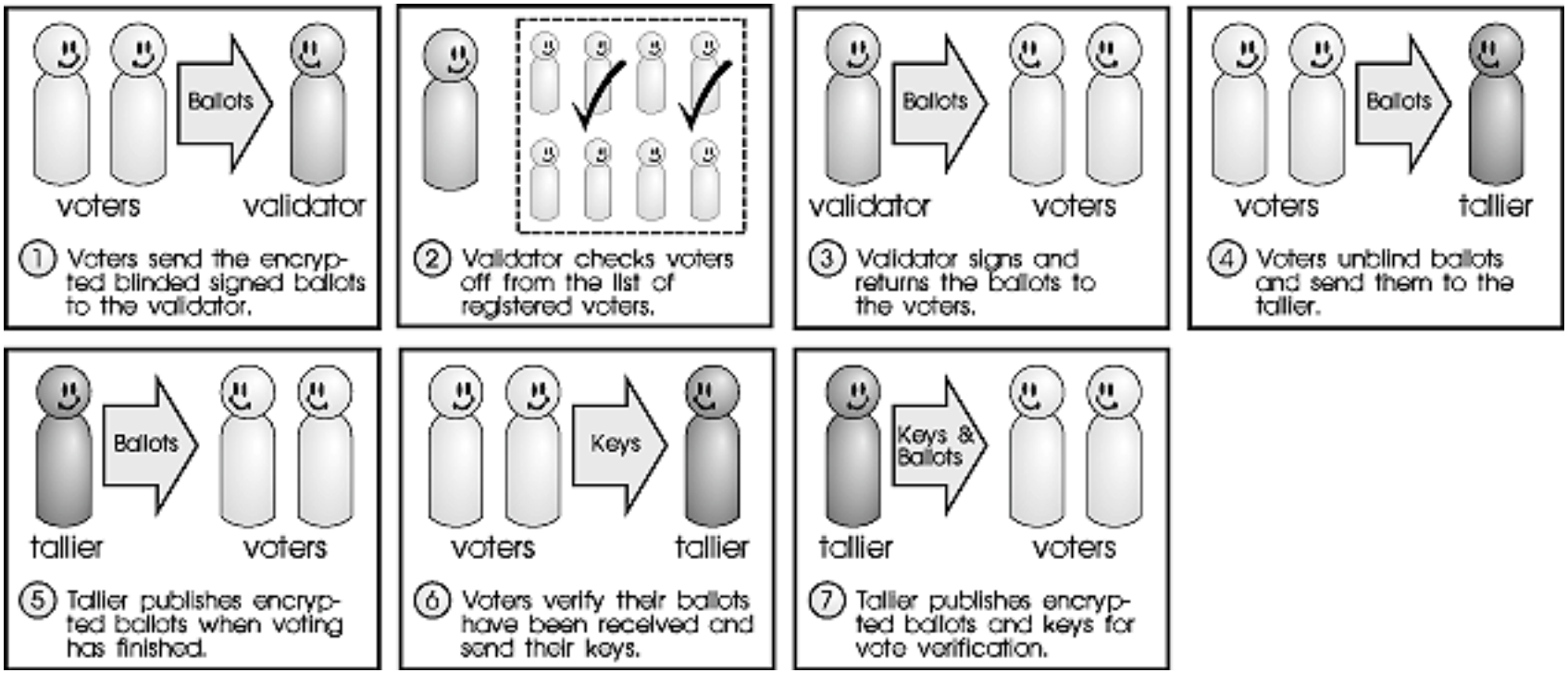
- Requires PKI
- Bad: compromised vote privacy if validator and tallier collude
- The Estonian system is based on such a scheme

Two-Agency Protocol (Salomaa, 91)



- Does not require PKI
- Good: protocol is verifiable by individual voters
- Bad: collusion between validator and tallier is still a problem
- Are the Geneva/Zürich systems based on such a scheme?

FOO92 Protocol



FOO92 Protocol (cont.)

- Requires PKI
- Blind signature guarantees vote privacy
- Individually and universally verifiable
- Problems:
  - → Validator may cast votes for abstaining voters (violates accuracy)
  - → The mechanism that allows voter to verify that their votes were counted also allows them to prove they voted in a particular way (violates receipt-freeness = allows vote buying)

References I

A. Aeby and M. Wiget.
On-Line Meinungsumfragen.

Diploma thesis, Bern University of Applied Sciences, Biel, Switzerland, 2007.

R. Anane, R. Freeland, and G. Theodoropoulos.
e-voting requirements and implementation.

In *CEC'07, 9th IEEE Conference on E-Commerce Technology*, pages 382–392, Tokyo, Japan, 2007.

F. Baiardi, A. Falleni, R. Granchi, F. Martinelli, M. Petrocchi, and A. Vaccarelli.
SEAS, a secure e-voting protocol: Design and implementation.

Computers & Security, 24(8):642–652, 2005.

References II

A. Baraani-Dastjerdi, J. Pieprzyk, and R. Safavi-Naini.
A practical electronic voting protocol using threshold schemes.

Technical report, University of Wollongong, Department of Computer Science, Wollongong, Australia, 1994.

D. Chaum.
Untraceable electronic mail, return addresses and digital pseudonyms.

Communications of the ACM, 24(2):84—88, 1981.

D. Chaum.
Blind signature system.

In *CRYPTO'83, 3rd International Cryptology Conference*, pages 153–156, Santa Barbara, USA, 1983.

References III

D. Chaum.
The dining cryptographers problem: Unconditional sender and recipient untraceability.

Journal of Cryptology, 1(1):65–75, 1988.

R. Cramer, R. Gennaro, and B. Schoenmakers.
A secure and optimally efficient multi-authority election scheme.

European Transactions on Telecommunications, 8(5):481–490, 1997.

References IV


L. F. Cranor and R. K. Cytron.
Sensus: A security-conscious electronic polling system for the internet.

In *HICSS-30, 30th Hawaii International Conference on System Sciences*, volume 03, pages 561–570, Maui, USA, 1997.


B. W. DuRette.
Multiple administrators for electronic voting.

Bachelor thesis, Massachusetts Institute of Technology, Boston, USA, 1999.

References V


A. Fujioka, T. Okamoto, and K. Ohta.
A practical secret voting scheme for large scale elections.
In J. Seberry and Y. Zheng, editors, *ASIACRYPT'92, Workshop on the Theory and Application of Cryptographic Techniques*, LNCS 718, pages 244–251, Gold Coast, Australia, 1992.


D. Goldschlag, M. Reed, and P. Syverson.
Onion routing for anonymous and private Internet connections.
Communications of the ACM, 42(2):39–41, 1999.


M. A. Herschberg.
Secure electronic voting using the world wide web.
Master's thesis, Massachusetts Institute of Technology, Boston, USA, 1997.

References VI

R. Joaquim, A. Zuquete, and P. Ferreira.
REVS – a robust electronic voting system.

In *IADIS International Conference e-Society 2003*, pages 95–103, Lisbon, Portugal, 2003.

A. Kiayias, M. Korman, and D. Walluck.
An internet voting system supporting user privacy.

In *ACSAC'06, 22nd Annual Computer Security Applications Conference*, pages 165–174, Miami Beach, USA, 2006.

K. Kim.
Killer application of PKI to internet voting.

In *IWAP'02, 2nd International Workshop for Asia Public Key Infrastructures*, Taipei, Taiwan, 2002.

References VII

R. Kofler, R. Krimmer, and A. Prosser.
Electronic voting: Algorithmic and implementation issues.
In *HICSS-36, 36th Annual Hawaii International Conference on System Sciences*, volume 5, pages 1–7, Waikoloa, USA, 2003.

V. Lehtonen.
Implementation of a robust electronic voting system.
Master's thesis, Helsinki University of Technology, Department of Computer Science and Engineering, Helsinki, Finland, 2001.

H. Nurmi, A. Salomaa, and L. Santean.
Secret ballot elections in computer networks.
Computers and Security, 10(6):553–560, 1991.

References VIII

M. Ohkubo, F. Miura, M. Abe, A. Fujioka, and T. Okamoto.
An improvement on a practical secret voting scheme.

In M. Mambo and Y. Zheng, editors, *ISW'99, 2nd International Workshop on Information Security*, LNCS 1729, pages 225–234, Kuala Lumpur, Malaysia, 1999.

T. Okamoto.
An electronic voting scheme.

In N. Terashima and E. Altman, editors, *IFIP World Conference on IT Tools*, pages 21–30, Canberra, Australia, 1996.

References IX

T. Okamoto.
Receipt-free electronic voting schemes for large scale elections.
In *5th International Security Protocols Workshop*, LNCS 1361, pages 25–35, Paris, France, 1997.

I. Ray, I. Ray, and N. Narasimhamurthi.
An anonymous electronic voting protocol for voting over the internet.
In *WECWIS'01, 3rd International Workshop on Advanced Issues of E-Commerce and Web-Based Information Systems*, pages 188–191, San Jose, USA, 2001.

References X


A. Riera and J. Borrell.
Practical approach to anonymity in large scale electronic voting schemes.
In *NDSS'99, Network and Distributed System Security Symposium*, pages 69–82, San Diego, USA, 1999.


G. Røsland.
Remote electronic voting.
Hovedoppgave, University of Bergen, Norway, 2004.


A. Salomaa.
Verifying and recasting secret ballots in computer networks.
In H. A. Maurer, editor, *New Results and New Trends in Computer Science*, LNCS 555, pages 283–289, Graz, Austria, 1991.