Crittografia avanzata
Lezione del 1 Giugno 2011

Bit commitment

- Pari o dispari?
  - Se Alice e Bob sono presenti, non ci sono problemi:
    - Alice sceglie
    - Bob lancia e si controlla
  - Se Alice non è presente:
    - Alice sceglie, “imbusta” la scelta e la manda a Bob
    - Bob lancia e manda il risultato ad Alice
    - Alice invia a Bob la chiave della busta
  - L'essenziale è che ci sia un'unica chiave per la busta
  - La “zero-knowledge proof è un altro esempio

Qual'è lo scopo del voto elettronico?

Qual'è lo scopo del voto elettronico?

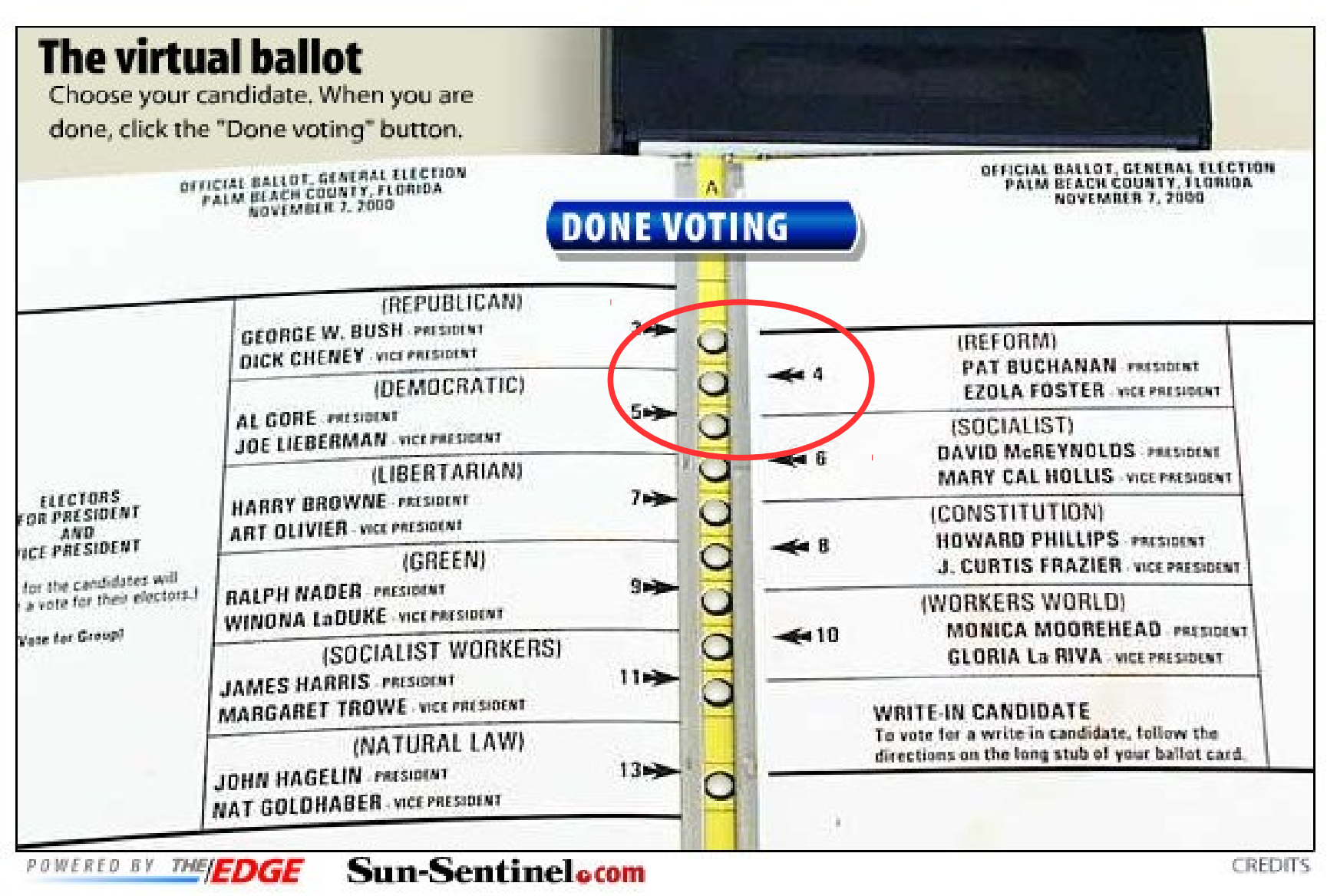
- Ridurre i costi
- Velocizzare i tempi
- Ridurre gli errori
- Ridurre le frodi
- Verifica diretta da parte dell'elettore
- Offrire opportunità maggiori
  - Diverse forme di voto
  - Votazioni più frequenti
  - Democrazia diretta
- Permettere il voto da casa
- … altro?

Il processo di voto in Italia

Il caso: le elezioni in Florida del 2000

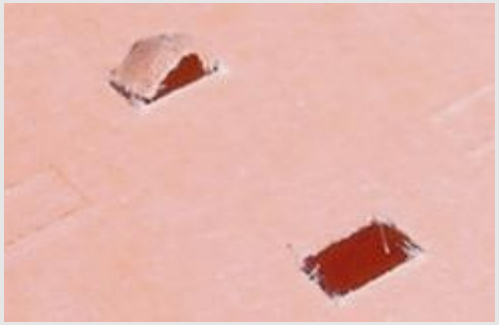
- Venivano utilizzate delle schede “perforate” dall'elettore mediante un'apposita macchina, lette da un lettore di schede perforate
- Vantaggi:
  - Voti chiaramente assegnati a un candidato...?
  - Schede bianche chiaramente riconoscibili...?
  - Spoglio veloce e “senza errori”
  - Riduzione delle frodi allo spoglio?

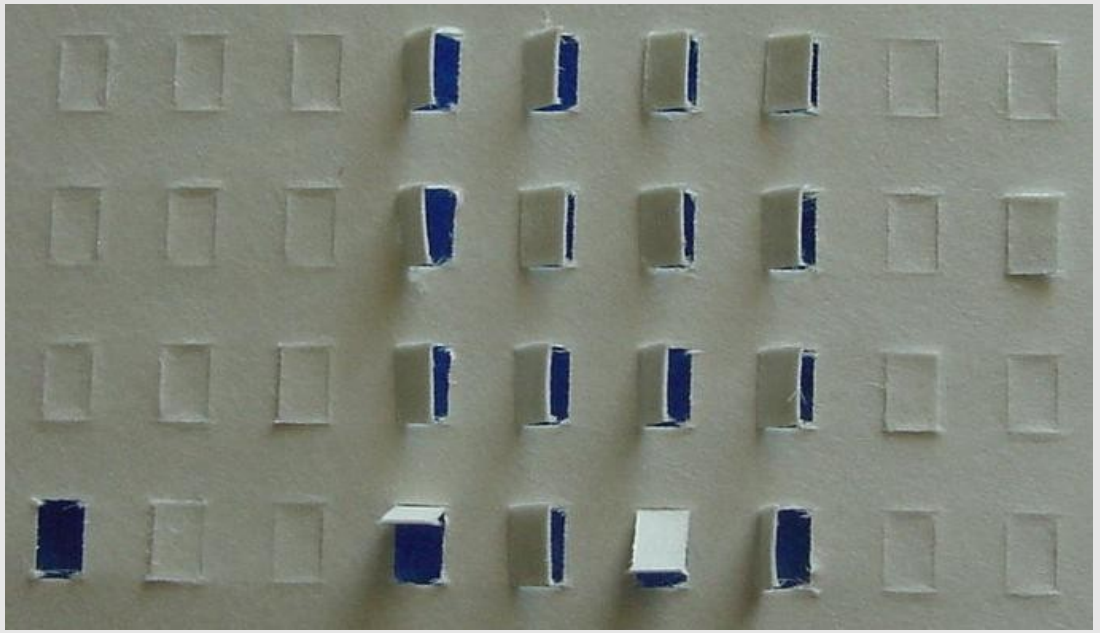
La scheda


The virtual ballot
Choose your candidate. When you are done, click the "Done voting" button.
OFFICIAL BALLOT, GENERAL ELECTION
PALM BEACH COUNTY, FLORIDA
NOVEMBER 7, 2000
DONE VOTING
OFFICIAL BALLOT, GENERAL ELECTION
PALM BEACH COUNTY, FLORIDA
NOVEMBER 7, 2000
ELECTORS FOR PRESIDENT AND VICE PRESIDENT
(Vote for the candidates will cast a vote for their electors.)
Vote for Group!
(REPUBLICAN)
GEORGE W. BUSH - PRESIDENT
DICK CHENEY - VICE PRESIDENT
3
(DEMOCRATIC)
AL GORE - PRESIDENT
JOE LIEBERMAN - VICE PRESIDENT
5
(LIBERTARIAN)
HARRY BROWNE - PRESIDENT
ART OLIVIER - VICE PRESIDENT
7
(GREEN)
RALPH NADER - PRESIDENT
WINONA LaDUKE - VICE PRESIDENT
9
(SOCIALIST WORKERS)
JAMES HARRIS - PRESIDENT
MARGARET TROWE - VICE PRESIDENT
11
(NATURAL LAW)
JOHN HAGELIN - PRESIDENT
NAT GOLDHABER - VICE PRESIDENT
13
4
(REFORM)
PAT BUCHANAN - PRESIDENT
EZOLA FOSTER - VICE PRESIDENT
6
(SOCIALIST)
DAVID McREYNOLDS - PRESIDENT
MARY CAL HOLLIS - VICE PRESIDENT
8
(CONSTITUTION)
HOWARD PHILLIPS - PRESIDENT
J. CURTIS FRAZIER - VICE PRESIDENT
10
(WORKERS WORLD)
MONICA MOOREHEAD - PRESIDENT
GLORIA La RIVA - VICE PRESIDENT
WRITE-IN CANDIDATE
To vote for a write-in candidate, follow the directions on the long stub of your ballot card.
POWERED BY THE EDGE
Sun-Sentinel.com
CREDITS

La macchina - Votomatic

Hanging chads





Frodi in Italia

- Le preferenze multiple
  - Covert channel per “codificare” il votante nell'ambito di voto di scambio
    - Possibile con un numero sufficiente di preferenze
    - Peggio potendo scrivere il nome
  - Abrogato nel corso di uno “storico” referendum del 1991
    - Ora è possibile una sola preferenza, con una croce
      - Dubbio: è possibile codificare il nome nella croce? “Knowledge is powe” insegna...

La scheda mancante

- Da un seggio “sparisce” una scheda
  - Qualcuno, es. uno scrutatore, la sottrae e la consegna al mafioso di turno, che ci mette il voto scelto, e la consegna ad un votante da controllare
- Un votante entra al seggio, riceve una scheda bianca
  - Nella cabina tirafuori la scheda precompilata, e mette in tasca quella bianca, poi mette nell'urna quella precompilata ed esce, consegnando quella bianca al mafioso
- In questo modo il mafioso può controllare direttamente un numero di voti dipendente solo dal tempo necessario per effettuare materialmente il voto

Cosa insegna la scheda mancante?

- Molti sistemi/modelli funzionano solo se le condizioni sono rispettate perfettamente, ma se qualcosa di “piccolo” nelle condizioni viene a mancare, crollano completamente
  - Non hanno ridondanza nelle protezioni (in quella fase)
  - Nella valutazione di sistemi reali è sempre da considerare
    - Analogo al problema dell'errore nella memoria della smart card
- Rimedio? Cosa si fa se al conteggio manca una scheda?
  - Anche sui rimedi, verificare che il modello sia realistico

La foto con il cellulare

- Il votante nella cabina elettorale e fotografa la scheda compilata prima di metterla di uscire
- Possibile anche con lo schermo di un computer...
- Dal 2003 il Viminale ha vietato l'ingresso di macchine fotografiche e simili nei seggi
  - Ma manca la possibilità di controllare
  - Episodio recente riportato alle Amministrative, il presidente di seggio ha sentito lo scatto (!!) ed ha chiamato i carabinieri

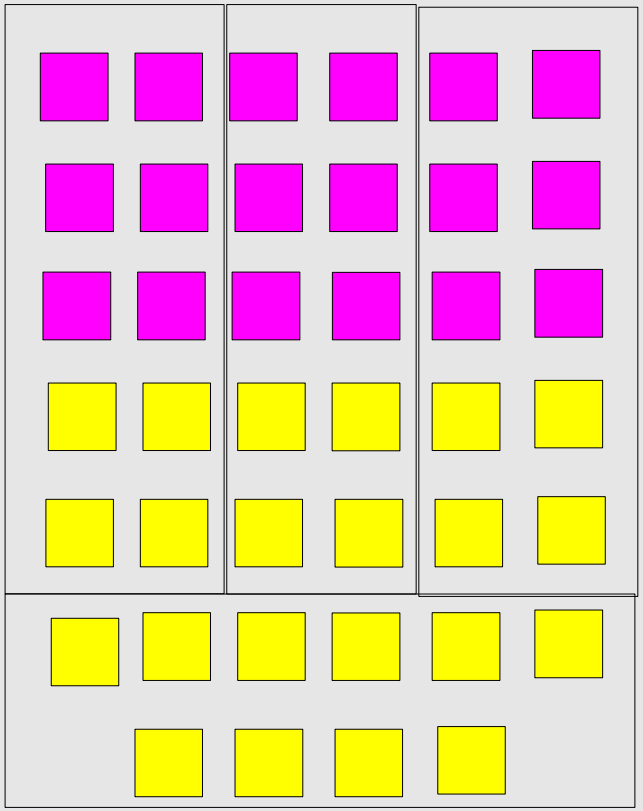
Mina sotto l'unghia...

- Uno scrutatore “esamina” una scheda e intanto traccia una x approssimativa su una scheda bianca
- Può essere confusa ad es. con il voto di un anziano...
- Può anche essere usato per invalidare una scheda, segnando una seconda x

Altri problemi

- Assalto al seggio
  - Problema reale ad es. in India
- Sorveglianza (voto da casa)
- Collusione del personale al seggio
- Manipolazione delle schede durante lo scrutinio
- Definizione dei collegi
- ...

Definizione dei collegi



I gialli sono di più, ma vincono
i rosa (o hanno più rappresentanti)
In alcuni paesi o casi storici, lo stesso effetto è stato ottenuto spostando la popolazione

Qual'è il modello delle minacce?

- Prima di discutere una qualsiasi “soluzione”, bisogna avere chiaro il problema
- Molte discussioni sul voto elettronico partono dalla “necessità” del voto elettronico, dal fatto che sia “un miglioramento”, senza discutere realmente né minacce né requisiti
- Coercizione
  - Soprattutto a mostrare il voto da parte dell'elettore, ma ovviamente non sulle terze parti
  - Deniable encryption

Aspetti tecnologici

- Prima di ragionare sui protocolli crittografici, parliamo di come si implementa il voto elettronico
- Prima distinzione: voto da casa vs. voto in seggio
  - Il voto da casa in altri paesi è diffuso (anche via posta tradizionale)
- Diverse fasi automatizzabili; principalmente
  - Voto
  - Scrutinio

Garanzie sugli apparati

- È il problema più sentito
  - Processi di certificazione
  - Complessità
  - Uso di strumenti COTS: svantaggio o vantaggio?
  - Metodi di verifica (es. a campione)
- Olanda e Tempest
- Gli apparati indiani
- I molti casi USA
- … nel complesso, ci si riallontana dai *direct-recording electronic voting systems*, o DRE

Auditabilità

- Chi è in grado di capire/verificare il sistema di voto e il voto?
- Se lo possono fare solo alcuni tecnici, il cittadino sta delegando una capacità che per ora ha
  - Non direttamente ma tramite es. rappresentanti di lista, che però non devono avere una cultura particolare
  - Quanto è verificabile a posteriori il voto?
    - Elezioni del 2006

Non funziona!

- Problema sottovalutato ma molto reale:
  - L'elettore entra nella cabina elettorale dotata di un “apparato”, e grida che l'apparato non funziona
    - Lui ha votato per uno, ma l'apparato ha votato per un altro
    - Come verificare mantenendo la segretezza del voto?
    - Come verificare su quanto già votato?
  - Il problema si è già posto in elezioni in USA
    - Soluzione molto pragmatica, praticabile negli USA ma probabilmente non dappetutto...
- In generale: cosa fare in caso di dubbi/errori?
  - Annullare tutta la consultazione è una soluzione “corretta” ma poco praticabile...

Requisiti di un sistema di voto (elettronico)

- privacy
- eligibility
- uniqueness
- fairness
- uncoercibility
- Receipt-freeness
- accuracy
- individual verifiability
- … ma il contesto e le minacce spesso non vengono definiti

Metodo Mercuri

- Paper-verified ballot
- Il votante vota attraverso una macchina
- La macchina stampa una scheda e la mostra al votante sotto a un vetro
- Se il votante è d'accordo, la macchina:
  - Fa cadere la scheda in un'urna
  - Registra elettronicamente il voto
- La carta è usata come strumento di verifica

Segretezza del voto

- Quando si valuta la segretezza del voto, bisogna considerare tutto quello che può portare ad associare il voto alla persona:
  - Marcature sulle schede (es. al momento della stampa) anche solo del numero della scheda (il nome è poi associabile tramite i registri)
  - Numeri di serie
  - Manipolazione della scheda dopo il voto

End-to-end auditable voting systems

- Prevedono per il votante la possibilità di verificare che il suo voto sia stato contato
  - Di solito al votante viene data una ricevuta; il suo voto viene pubblicato e lui può controllare e contestare, ma non se ne deduce per chi ha votato
  - Attenzione alle terze parti fidate:
    - Nel setup
    - Nell'audit
- Le Terze parti sono molto fidate, perché il votante non ha modo di dedurre la correttezza delle operazioni, data la forte componente crittografica

Alcuni sistemi di voto

- Prête-a-voter
  - Nessun utilizzo di crittografia
- Puchscan/scantegrity
  - Verificabile “pubblicamente”. Ma con trusted third parties
- OpenVote

E la macchina fotografica?

- In teoria il metodo Mercuri permette di fare una foto e poi annullare il voto e rifarlo
- In pratica la doppia votazione si “sente”
- Fotografare lo schermo o la scheda è quasi sempre possibile
- Soluzioni?

Forse può aiutare?