

Il voto elettronico: le elezioni del futuro o il rischio della democrazia?

Simone Martini

Dipartimento di Scienze dell'Informazione
Alma mater studiorum • Università di Bologna

Riflessioni su Scienza e Società – Bologna, 7 aprile 2011

Il voto segreto

- Dal voto palese alla scheda
- Cuore della democrazia liberale post-illuminista
- Solo modo di espressione della volontà popolare in sede istituzionale
- Istituzioni validamente costituite

Le garanzie

- Un voto (al più) per ogni testa
- Definitività
- Segretezza:
 - il voto è segreto
 - nessuno è in grado di “dire” come un elettore ha votato neppure l'elettore stesso (cfr incoercibilità)
- Integrità:
 - i voti sono contati per quello che sono
 - i conteggi sono accurati
- Verificabilità: l'integrità dei conteggi può essere verificata
- Disponibilità; usabilità; accessibilità

Le garanzie

- Un voto (al più) per ogni testa
- Definitività
- Segretezza:
 - il voto è segreto
 - nessuno è in grado di “dire” come un elettore ha votato neppure l'elettore stesso (cfr incoercibilità)
- Integrità:
 - i voti sono contati per quello che sono
 - i conteggi sono accurati
- Verificabilità: l'integrità dei conteggi può essere verificata
- Disponibilità; usabilità; accessibilità

Il voto con la scheda

- Una testa, un voto: liste e certificati elettorali
- Privacy:
 - segreto: cabina, divieti (cellulari, foto, etc.)
 - indimostrabile: non ci sono ricevute, divieti
- Definitività: urna
- Integrità: seggio elettorale, procedure, rappresentanti
- Verificabilità: ricalcolo sui riassunti o sulle schede originali
- Disponibilità; usabilità; accessibilità: ...

Patologie, 1

Elezioni politiche 25 marzo 1934



Per votare **NO** occorre
ritirare un'altra scheda

Patologie, 1

Elezioni politiche 25 marzo 1934



Per votare **NO** occorreva ritirare un'altra scheda

Preferenze multiple

- Fissato un candidato Tizio da far votare
- Con 4 preferenze possibili
- Su una lista di 20 candidati
- Ci sono $4 \cdot 19 \cdot 18 \cdot 17 = 23\ 256$ disposizioni diverse di 4 preferenze
- In un seggio votano **molto meno** di 20 000 elettori
- Spontaneamente, pochi elettori usano 4 preferenze

- La combinazione è una **firma**
- Consente di verificare con buona approssimazione che X ha votato Tizio

La scheda è robusta

- Nonostante le possibili distorsioni
- Resistente a piccole perturbazioni
- Brogli estesi solo con ampio coinvolgimento di diversi attori
- Difficile influenzare elezioni su vasta scala
- È importante la **catena di custodia**

Tutto a mano?

- Tutto a mano nei singoli seggi
- Trasmissione digitale telematica (sicura?)
- Aggregazione automatica (corretta?)

Errori nel processo automatico?

- Possibili
- Possibili anche in malafede
- Autorità indipendenti tra loro (commissioni elettorali) ricalcolano i vari aggregati
- Pubblicazione dei dati
 - aggregati
 - disaggregati
 - per singoli seggi
- Audit dei programmi utilizzati
- Extrema ratio: ricalcolo sulle schede originali

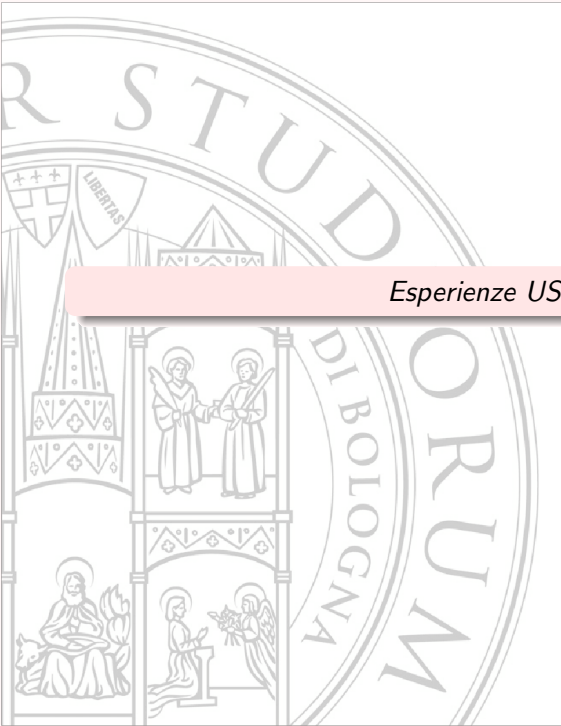
Errori nel processo automatico?

- Possibili
- Possibili anche in malafede
- Autorità indipendenti tra loro (commissioni elettorali) ricalcolano i vari aggregati
- **Pubblicazione dei dati**
 - aggregati
 - disaggregati
 - per singoli seggi
- **Audit** dei programmi utilizzati
- **Extrema ratio**: **ricalcolo sulle schede originali**

Errori nel processo automatico, 2

La catena di custodia delle comunicazioni

- Trasmissione dalla periferia al centro
- Aggregazione dei dati
- Come garantire sicurezza dei processi informatici e telematici coinvolti?
- Trasparenza
- Audit
- Coinvolgimento di terze parti

The background of the slide features a large, light-colored watermark of the official seal of the University of Bologna. The seal is circular and contains the text 'R STUD' at the top and 'DI BOLOGNA' and 'ORUM' at the bottom. In the center, there are several figures: two standing figures holding a banner, a seated figure with a dog, and a kneeling figure with an angel. A shield with a cross and the word 'LIBERTAS' is also visible.

Esperienze USA

L'evoluzione del voto USA

- Scheda
- Macchine meccaniche a leve
- Macchine (elettro-)meccaniche perforatrici
- Scan ottico
- Voto elettronico diretto
DRE: Direct Recording by Electronics, touchscreen
- DRE + copia cartacea (DRE+VVPAT)

- Voto per posta
- Voto via web

- End-to-end voting

L'evoluzione del voto USA

- Scheda
- Macchine meccaniche a leve
- Macchine (elettro-)meccaniche perforatrici
- Scan ottico
- Voto elettronico diretto
DRE: Direct Recording by Electronics, touchscreen
- DRE + copia cartacea (DRE+VVPAT)

- Voto per posta
- Voto via web

- End-to-end voting

L'evoluzione del voto USA

- Scheda
- Macchine meccaniche a leve
- Macchine (elettro-)meccaniche perforatrici
- Scan ottico
- Voto elettronico diretto
DRE: Direct Recording by Electronics, touchscreen
- DRE + copia cartacea (DRE+VVPAT)

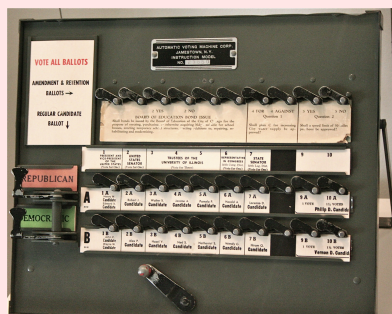
- Voto per posta
- Voto via web

- End-to-end voting

La macchina a leve



La macchina a leve, 2



- Circa 1892 — 1982.
- Semplice costruzione meccanica
- Non preserva il singolo voto, ma solo l'aggregato

Voto perforato



In uso da circa il 1960.

Nel 2002 lo **Help America Vote Act** le rende illegali.

Scheda per voto perforato

DO NOT DETACH STUB-FOLD OVER

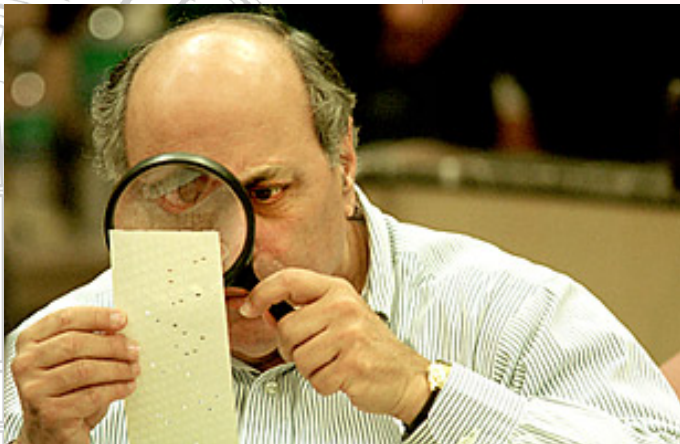
1	•	40	•	97	•	136	•	166	•	178	•	199	•	216								
2	•	21	•	59	•	78	•	98	•	118	•	137	•	157	•	177	•	197	•	217		
3	•	22	•	41	•	60	•	79	•	99	•	119	•	138	•	158	•	178	•	198	•	218
4	•	23	•	42	•	61	•	80	•	99	•	119	•	138	•	158	•	178	•	198	•	218
5	•	24	•	43	•	62	•	81	•	100	•	120	•	139	•	159	•	179	•	199	•	219
6	•	25	•	44	•	63	•	82	•	101	•	121	•	140	•	160	•	180	•	200	•	220
7	•	26	•	45	•	64	•	83	•	102	•	122	•	141	•	161	•	181	•	201	•	221
8	•	27	•	46	•	65	•	84	•	103	•	123	•	142	•	162	•	182	•	202	•	222
9	•	28	•	47	•	66	•	85	•	104	•	124	•	143	•	163	•	183	•	203	•	223
10	•	29	•	48	•	67	•	86	•	105	•	125	•	144	•	164	•	184	•	204	•	224
11	•	30	•	49	•	68	•	87	•	106	•	126	•	145	•	165	•	185	•	205	•	225
12	•	31	•	50	•	69	•	88	•	107	•	127	•	146	•	166	•	186	•	206	•	226
13	•	32	•	51	•	70	•	89	•	108	•	128	•	147	•	167	•	187	•	207	•	227
14	•	33	•	52	•	71	•	90	•	109	•	129	•	148	•	168	•	188	•	208	•	228
15	•	34	•	53	•	72	•	91	•	110	•	130	•	149	•	169	•	189	•	209	•	229
16	•	35	•	54	•	73	•	92	•	111	•	131	•	150	•	170	•	190	•	210	•	230
17	•	36	•	55	•	74	•	93	•	112	•	132	•	151	•	171	•	191	•	211	•	231
18	•	37	•	56	•	75	•	94	•	113	•	133	•	152	•	172	•	192	•	212	•	232
19	•	38	•	57	•	76	•	95	•	114	•	134	•	153	•	173	•	193	•	213	•	233
20	•	39	•	58	•	77	•	96	•	115	•	135	•	154	•	174	•	194	•	214	•	234
	•	40	•	59	•	78	•	97	•	116	•	136	•	155	•	175	•	195	•	215	•	235

TO BE FILLED IN BY COUNTING BOARD STAFF

PRECINCT NO. _____

MARKER NO. _____

Imprecisioni; difficile lettura



Butterfly ballot

1 OFFICIAL BALLOT, GENERAL ELECTION
PALM BEACH COUNTY, FLORIDA
NOVEMBER 7, 2000

1 R OFFICIAL BALLOT, GENERAL ELECTION
PALM BEACH COUNTY, FLORIDA
NOVEMBER 7, 2000

ELECTORS FOR PRESIDENT AND VICE PRESIDENT	
(REPUBLICAN)	
GEORGE W. BUSH - PRESIDENT	3 →
DICK CHENEY - VICE PRESIDENT	
(DEMOCRATIC)	
AL GORE - PRESIDENT	5 →
JOE LIEBERMAN - VICE PRESIDENT	
(LIBERTARIAN)	
HARRY BROWNE - PRESIDENT	7 →
ART OLIVIER - VICE PRESIDENT	
(GREEN)	
RALPH NADER - PRESIDENT	9 →
WINONA LA DUKE - VICE PRESIDENT	
(SOCIALIST WORKERS)	
JAMES HARRIS - PRESIDENT	11 →
MARGARET TROWE - VICE PRESIDENT	
(NATURAL LAW)	
JOHN HAGELIN - PRESIDENT	13 →
NAT GOLDHABER - VICE PRESIDENT	

(A vote for the candidates will actually be a vote for their electors.)
(Vote for Group)

← 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.			

TURN PAGE TO CONTINUE VOTING →

Al Gore è il **secondo** candidato;
ma deve essere perforato il **terzo** foro.

Scan ottico

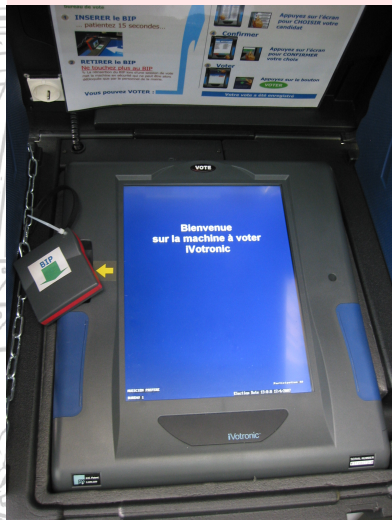
Simile al voto perforato ma scheda ottica; in uso dal 1962.
Conteggio centralizzato o **per seggio** (*precint*).

Scan ottico, 2

Precinct Counted Optical Scan, PCOS

- L'elettore annerisce il proprio voto
- Inserisce la scheda nella macchina
- La macchina segnala eventuale nullità (overvote, undervote)
- Calcolo automatico dei totali
- Le schede sono preservate in urne sigillate
- Possibilità di ricalcolo e audit
- Forte dipendenza dalla catena di custodia delle macchine

Direct Recording by Electronics



Analogo a scan ottico, ma su touch screen.

Primo uso circa 1980.

Direct Recording by Electronics

DRE

- Uso di hardware e SO standard (PC, Windows)
- Scheda non preservata
- Come è garantita la segretezza?
- Difficile verifica di molti aspetti da parte dei pubblici ufficiali
- Catena di custodia fuori della portata dei pubblici ufficiali

Letteratura su DRE

Concorde nel rilevare:

- possibilità (e talvolta anche semplicità) di attacchi maliziosi
- difficoltà di assicurare una catena di custodia corretta
- impossibilità per molti attori di accedere ai dettagli delle macchine

P.e.

Insecurities and Inaccuracies of the Sequoia AVC Advantage 9.00H DRE Voting Machine

Andrew W. Appel*
Princeton University

Maia Ginsburg
Princeton University

Harri Hursti

Brian W. Kernighan
Princeton University

Christopher D. Richards
Princeton University

Gang Tan
Lehigh University

October 17, 2008

Letteratura su DRE

Concorde nel rilevare:

- possibilità (e talvolta anche semplicità) di attacchi maliziosi
- difficoltà di assicurare una catena di custodia corretta
- impossibilità per molti attori di accedere ai dettagli delle macchine

P.e.

Insecurities and Inaccuracies of the Sequoia AVC Advantage 9.00H DRE Voting Machine

Andrew W. Appel*
Princeton University

Maia Ginsburg
Princeton University

Harri Hursti

Brian W. Kernighan
Princeton University

Christopher D. Richards
Princeton University

Gang Tan
Lehigh University

October 17, 2008

Executive Summary. The Sequoia AVC Advantage is a direct-recording electronic (DRE) voting machine used in New Jersey, Pennsylvania, and other states.

I. The AVC Advantage 9.00 is easily “hacked,” by the installation of fraudulent firmware. This is done by prying just one ROM chip from its socket and pushing a new one in, or by replacement of the Z80 processor chip. We have demonstrated that this “hack” takes just 7 minutes to perform.

The fraudulent firmware can steal votes during an election, just as its criminal designer programs it to do. The fraud cannot practically be detected. There is

II. Without even touching a single AVC Advantage, an attacker can install fraudulent firmware into many AVC Advantage machines by viral propagation through audio-ballot cartridges. The virus can steal the votes of blind voters, can cause AVC Advantages in targeted precincts to fail to operate; or can cause WinEDS software to tally votes inaccurately.

III. Design flaws in the user interface of the AVC Advantage disenfranchise voters, or violate voter privacy, by causing votes not to be counted, and by allowing pollworkers to commit fraud.

IV. AVC Advantage Results Cartridges can be easily manipulated to change votes, after the polls are closed but before results from different precincts are cumulated together.

V. Sequoia’s sloppy software practices can lead to error and insecurity. Wyle’s ITA reports are not rigorous, and are inadequate to detect security vulnerabilities. Programming errors that slip through these processes can miscount votes and permit fraud.

In sostanza

Un DRE:

- Contiene molto software:
 - alcune centinaia di migliaia di righe
più il sistema operativo
- Il sw difficile da scrivere, testare, valutare
- È difficile garantire l'integrità del sistema hw+sw
- Difficile assicurare insieme segretezza, integrità e verificabilità

DRE+copia cartacea

DRE + VVPAT



Primo uso nel 2003

L'elettore **vede** anche una scheda cartacea

Elettore conferma la scheda

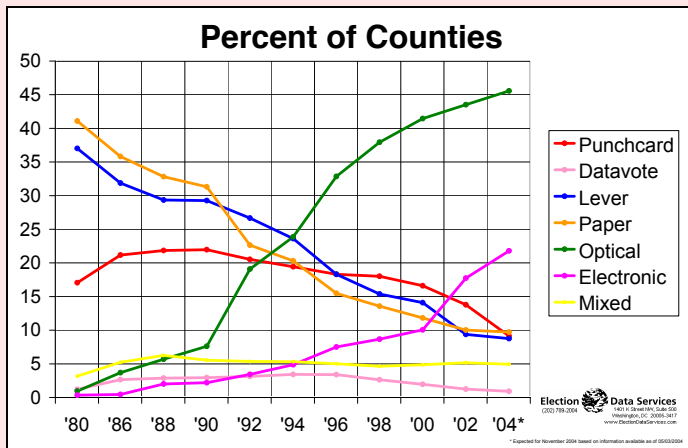
La scheda è conservata in un'urna sigillata

La copia cartacea permette:

- all'elettore di verificare **senza affidarsi al software** che esiste una registrazione corretta del proprio voto
- Ricalcoli
- **Audit**: confronto tra campionamenti statistici delle schede cartacee e gli aggregati ottenuti automaticamente.

Il declino della scheda

USA



Riassumendo: voto elettromeccanico o elettronico

- La verifica della correttezza è delegata ai pubblici ufficiali
- La verifica dipende fortemente dalla catena di custodia
- Il ripristino (*recovery*) è molto difficile
 - meccanismi di controllo rari e a grana grossa;
 - rilevano più errori in buona fede che attacchi maliziosi
 - difficile, talvolta impossibile, ripristinare uno stato corretto in presenza di rilevata infrazione
- Audit statistico essenziale (e progettato ad hoc).

The Brennan Center Report

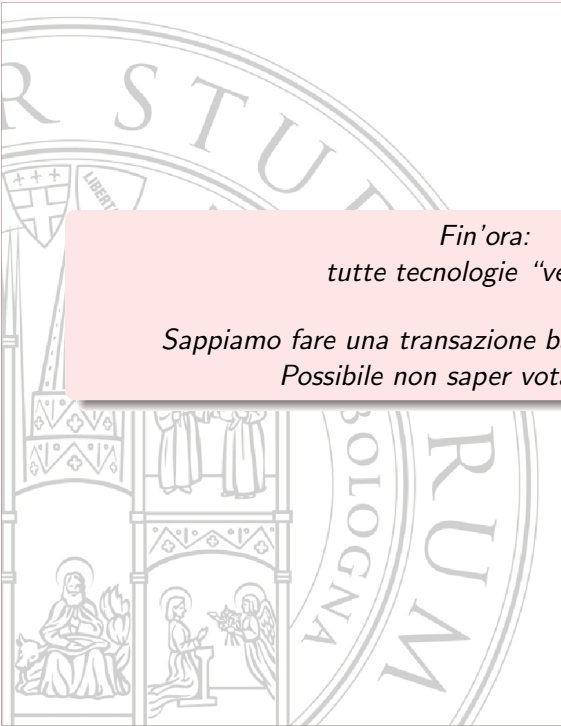
- 1 *All of the most commonly purchased electronic voting systems – DREs, DREs w/ VVPT, and PCOS – have significant security and reliability vulnerabilities, which pose a real danger to the integrity of national, state, and local elections.*
- 2 *The most troubling vulnerabilities of each system can be substantially remedied if proper countermeasures are implemented at the state and local level.*
- 3 *Few jurisdictions have implemented any of the key countermeasures that could make the least difficult attacks against voting systems much more difficult to execute successfully.*

BRENNAN CENTER
FOR JUSTICE

at New York University School of Law

Altri “metodi”

- Voto per posta
- Voto via web
- Non garantiscono segretezza e incoercibilità
- Sono metodi accettabili solo in casi molto limitati in cui si possa accettare la semplicità rinunciando alla segretezza
- Certo non per eleggere istituzioni locali o nazionali



*Fin'ora:
tutte tecnologie "vecchie"*


*Sappiamo fare una transazione bancaria **sicura** online
Possibile non saper votare online?*

Transazioni bancarie

- Molto più semplici del voto
- Ricevuta
- Attacchi più definiti
- Nel voto elettronico **tutti gli attori** sono potenzialmente in malafede

End-to-end Voting

- Protocollo di voto e tecnologie di sicurezza
- Che permettano ad **ogni singolo elettore** di verificare che il proprio voto sia
 - espresso come voluto
 - registrato come espresso
 - conteggiato come registrato
- Usando tecnologie crittografiche per garantire la privacy del voto
- Correttezza, segretezza, ecc.
non dipendono dalla catena di custodia
- O anche: la catena di custodia è verificabile da ogni utente

The background of the slide features a large, faint watermark of the seal of the University of Bologna. The seal is circular and contains the text "R STUD" at the top, "DI BOLOGNA" on the left, and "ORUM" at the bottom. The central part of the seal depicts a building with a tower and a shield with a cross and three stars, and the word "LIBERTAS" written on a banner. Below the building are two scenes: one showing a seated figure with a dog and another showing a kneeling figure and a standing figure.

Alcune tecnologie di crittografia

Crittografia tradizionale

Crittografia simmetrica a chiave privata

- Alice vuole comunicare M a Bob
- Alice e Bob condividono una chiave k
- Alice manda $T = F_k(M)$
- Bob ricava $M = F_k^{-1}(T)$
- Occorre un canale sicuro per lo scambio preliminare di k

Crittografia asimmetrica

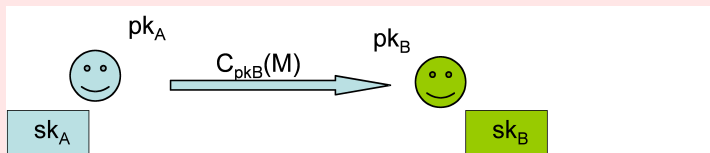
Diffie e Hellman, 1976

- Alice vuole comunicare M a Bob
- Alice ha due chiavi: pk_A (pubblica) e sk_A (segreta)
- Bob ha due chiavi: pk_B (pubblica) e sk_B (segreta)
- Le chiavi pubbliche sono. . . pubbliche
- Le chiavi segrete sono note solo al loro possessore

Crittografia asimmetrica

Diffie e Hellman, 1976

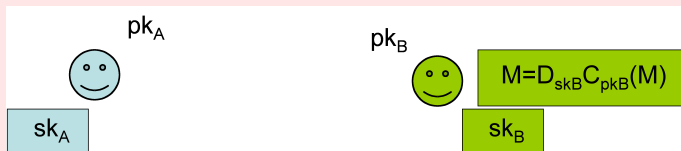
- Alice vuole comunicare M a Bob
- Alice ha due chiavi: pk_A (pubblica) e sk_A (segreta)
- Bob ha due chiavi: pk_B (pubblica) e sk_B (segreta)
- Le chiavi pubbliche sono. . . pubbliche
- Le chiavi segrete sono note solo al loro possessore



Crittografia asimmetrica

Diffie e Hellman, 1976

- Alice vuole comunicare M a Bob
- Alice ha due chiavi: pk_A (pubblica) e sk_A (segreta)
- Bob ha due chiavi: pk_B (pubblica) e sk_B (segreta)
- Le chiavi pubbliche sono. . . pubbliche
- Le chiavi segrete sono note solo al loro possessore



Crittografia asimmetrica

Ovvero:

- Alice manda a Bob $T = C_{pk_B}(M)$
- Bob ricava $M = D_{sk_B}^{-1}(T)$
- Le due funzioni di codifica C_{pk_B} e decodifica D_{sk_B} sono inverse ma:

Il calcolo di C_{pk_B} è facile

Il calcolo di D_{sk_B} è facile se sk_B è noto

Altrimenti il calcolo di D_{sk_B} è **difficile**

Senza pk_B , $T = C_{pk_B}(M)$ non rivela nulla su M .

Schemi a chiave pubblica

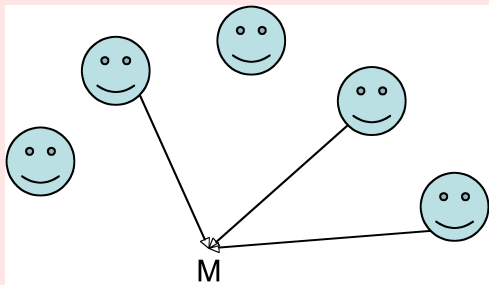
Scegliere \mathcal{C} e \mathcal{D}

- Basati su proprietà di teoria dei numeri (primalità, gruppi, campi, ecc.)
- RSA [Rivest, Shamir, Adleman, 1978]
 - la **fattorizzazione** di un numero è considerato **difficile**
 - test di primalità è facile
- El Gamal [1985]
- Curve ellittiche [1985]
- Pailler [1999]
- ...

Secret sharing

- Un dato D è diviso in n pezzi
- D è facilmente ricostruibile a partire da k pezzi
- Ma la completa conoscenza di $k - 1$ pezzi (qualunque) **non rivela alcunché** su D .

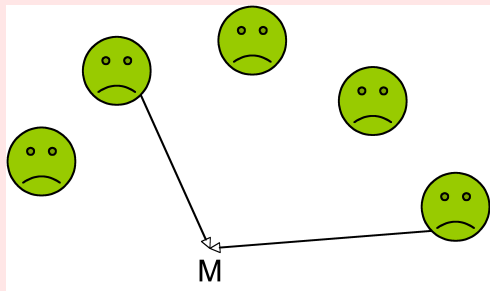
[Shamir 1979]



Secret sharing

- Un dato D è diviso in n pezzi
- D è facilmente ricostruibile a partire da k pezzi
- Ma la completa conoscenza di $k - 1$ pezzi (qualunque) **non rivela alcunché** su D .

[Shamir 1979]



Sistemi a soglia

Generalizzano la tecnica di Shamir

- La chiave segreta di decodifica non è posseduta da nessuno
- Invece, n persone possiedono ciascuna una porzione sk_n
- Se almeno k chiavi sono usate insieme è possibile decodificare
- Mentre $k - 1$ chiavi non rivelano alcunché
- Le chiavi segrete possono essere generate in modo indipendente
- Nessuno è a conoscenza dell'intera chiave sk .

Scantegrity II

Un sistema E2E:

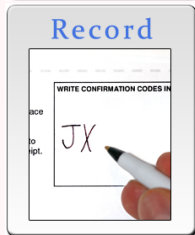
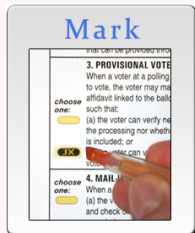
- Si associa ad uno scan ottico
- Lo scan ottico può essere usato “come prima”
- Scantegrity II aggiunge un livello di verifica E2E
- Basato su tecniche crittografiche che assicurano privacy e verificabilità

[Chaum et al. 2008]

Scantegrity II

La vista dell'elettore

- Vota su scheda di carta (ide seriale)
- Lo specifico voto rivela (inchiostro invisibile) un codice di controllo
- L'elettore (se vuole) annota seriale e codice di controllo ("espresso come voluto")
- La scheda è passata allo scan ottico, tabulata e conservata



Scantegrity II

Dopo la chiusura del voto...

- Le schede sono tabulate normalmente via lo scan
- Sul web è pubblicata la lista dei seriali **insieme** ai relativi codici di controllo
- L'elettore può verificare che il suo seriale è stato contato con il suo codice ("registrato come espresso")



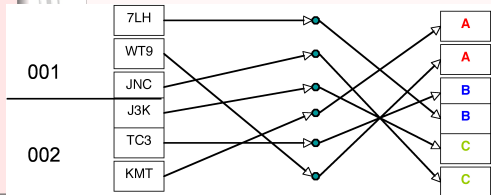
Il punto di vista del seggio

Prima del voto:

- il seggio **condivide segretamente** un seme di un generatore casuale
- che genera i codici di controllo, stampati sulle schede
Tabella P, segreta
- genera una prima permutazione dei codici, per seriale
- e due permutazioni che “mescolano” codici e candidati
le permutazioni non sono mai pubbliche contemporaneamente e intere

Ballot ID	Alice	Bob	Carl
0001	WT9	7LH	JNC
0002	KMT	TC3	J3K
0003	CH7	3TW	9JH
0004	WJL	KWK	H7T
0005	M39	LTM	HNN

Table P



Il punto di vista del seggio, 2

Prima del voto:

- il seggio **fissa definitivamente** valori e permutazioni
- e annuncia il proprio **commitment** su web

001	7LH	●	A
	WT9	●	A
	JNC	●	B
002	J3K	●	B
	TC3	●	C
	KMT	●	C

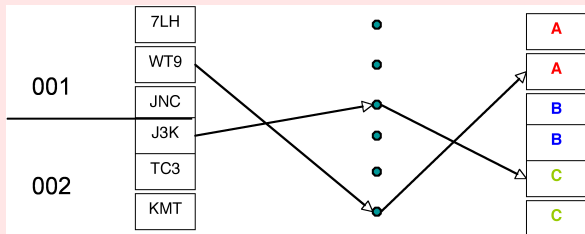
Commitment

- A **fissa** (*commits to*) una certa informazione i , senza rivelarla
- A comunica il suo **commitment** c a B
- B non è in grado di risalire ad i attraverso c
- Quando, in seguito, A rivela i a B, B può usare c per convincersi che A non ha modificato la sua scelta i .

Annuncio dei risultati

Dopo il voto:

- 001 ha un voto per Alice: WT9
- 002 ha un voto per Carl: J3K
- La doppia permutazione viene applicata ai voti
- Solo il risultato della permutazione è visibile
- I dettagli sono nascosti dalla crittografia



Annuncio dei risultati

Dopo il voto:

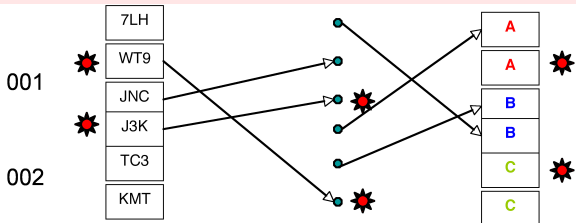
- 001 ha un voto per Alice: WT9
- 002 ha un voto per Carl: J3K
- La doppia permutazione viene applicata ai voti
- Solo il risultato della permutazione è visibile
- I dettagli sono nascosti dalla crittografia

001	7LH	●	A	★
	WT9	●	A	
	JNC	● ★	B	
002	J3K	●	B	
	TC3	●	C	★
	KMT	● ★	C	

Audit dei risultati

Randomized partial checking:

- Il mixnet viene aperto casualmente
- Solo una parte per riga
- Chiunque verifica che le marche sono propagate correttamente



Scantegrity II

- Necessita di hardware sicuro
- Codice open source, pubblico e disponibile
- Il codice serve per la verifica, non per il calcolo
- Alcune esperienze sul campo
elezioni comunali di Takoma Park, MD; meno di 2000 votanti

Concludendo

Sistemi E2E

- sembrano consentire “integrità verificabile”
- certo maggiore di quella dei sistemi attuali in uso
- **verifica del risultato vs verifica dell'hw e sw**
- ancora ricerca, test e sviluppo per
 - confirmare privacy
 - accessibilità
 - scalabilità
 - ecc.

COSTITUZIONE DELLA REPUBBLICA ITALIANA

TITOLO IV RAPPORTI POLITICI

ART. 48.

Sono elettori tutti i cittadini, uomini e donne, che hanno raggiunto la maggiore età.

Il voto è personale ed eguale, libero e segreto. Il suo esercizio è dovere civico.

Il diritto di voto non può essere limitato se non per incapacità civile o per effetto di sentenza penale irrevocabile o nei casi di indegnità morale indicati dalla legge.

Data a Roma, addì 27 dicembre 1947.

CONTRAFIRMANO:

Il Presidente dell'Assemblea Costituente

Giuseppe Macarone

Il Presidente del Consiglio dei Ministri

Giuseppe De Gasperi

Enrico De Nicola