Elektroniczna Demokracja
e-voting

prof. Mirosław Kutyłowski,
Marek Klonowski, Anna Lauks, Filip Zagórski

Sejm Rzeczypospolitej Polskiej

7 czerwca 2005

Wady tradycyjnego sposobu głosowania

- wysokie koszty
- brak weryfikowalności
- łatwość manipulacji przez komisje wyborcze

Sposoby oszukiwania

- unieważnianie głosów
  - przypadek Duval County, Floryda, Bush-Kerry 2004 niewytłumaczalna statystycznie zależność między liczbą unieważnionych głosów a procentem głosów na Kerrego

Sposoby oszukiwania

- unieważnianie głosów
  - przypadek Duval County, Floryda, Bush-Kerry 2004
    niewytłumaczalna statystycznie zależność między liczbą unieważnionych głosów a procentem głosów na Kerrego
- znikający atrament

  pióra w lokalach wyborczych, Ukraina, 2004

Sposoby oszukiwania

- unieważnianie głosów
  - przypadek Duval County, Floryda, Bush-Kerry 2004
    niewytłumaczalna statystycznie zależność między liczbą unieważnionych głosów a procentem głosów na Kerrego
- znikający atrament

  pióra w lokalach wyborczych, Ukraina, 2004
- składanie głosów za wyborców

  przypadki uznanych protestów wyborczych, wybory do Sejmu 2001

Inne problemy

- Wysyłanie głosów pocztą
  - czy kupowanie głosów, nierealne?

Inne problemy

- Wysyłanie głosów pocztą
  - czy kupowanie głosów, nierealne?
    - USA, NJ 2004, senator Jon Corzine wydał 65$ mln na kampanię, otrzymał 1.470 tys. głosów, co daje 44$ na głos.
    - Niemcy 2002, można było kupić paczkę 10.000 głosów za 59.000 EUR,

Inne problemy

- Wysyłanie głosów pocztą
  - czy kupowanie głosów, nierealne?
    - USA, NJ 2004, senator Jon Corzine wydał 65$ mln na kampanię, otrzymał 1.470 tys. głosów, co daje 44$ na głos.
    - Niemcy 2002, można było kupić paczkę 10.000 głosów za 59.000 EUR,
  - niszczenie głosów z określonych regionów
    (Broward County, Floryda, 2000 - 58.000 głosów zniknęło z urzędu pocztowego - hrabstwo z wyraźną przewagą Gore'a)

Inne problemy

- Wysyłanie głosów pocztą
  - czy kupowanie głosów, nierealne?
    - USA, NJ 2004, senator Jon Corzine wydał 65$ mln na kampanię, otrzymał 1.470 tys. głosów, co daje 44$ na głos.
    - Niemcy 2002, można było kupić paczkę 10.000 głosów za 59.000 EUR,
  - niszczenie głosów z określonych regionów (Broward County, Floryda, 2000 - 58.000 głosów zniknęło z urzędu pocztowego - hrabstwo z wyraźną przewagą Gore'a)
- Głosowanie przez internet

Inne problemy

- Wysyłanie głosów pocztą
  - czy kupowanie głosów, nierealne?
    - USA, NJ 2004, senator Jon Corzine wydał 65$ mln na kampanię, otrzymał 1.470 tys. głosów, co daje 44$ na głos.
    - Niemcy 2002, można było kupić paczkę 10.000 głosów za 59.000 EUR,
  - niszczenie głosów z określonych regionów (Broward County, Floryda, 2000 - 58.000 głosów zniknęło z urzędu pocztowego - hrabstwo z wyraźną przewagą Gore'a)
- Głosowanie przez internet
  - łatwość sprzedawania/kupowania głosów

Inne problemy

- Wysyłanie głosów pocztą
  - czy kupowanie głosów, nierealne?
    - USA, NJ 2004, senator Jon Corzine wydał 65$ mln na kampanię, otrzymał 1.470 tys. głosów, co daje 44$ na głos.
    - Niemcy 2002, można było kupić paczkę 10.000 głosów za 59.000 EUR,
  - niszczenie głosów z określonych regionów (Broward County, Floryda, 2000 - 58.000 głosów zniknęło z urzędu pocztowego - hrabstwo z wyraźną przewagą Gore'a)
- Głosowanie przez internet
  - łatwość sprzedawania/kupowania głosów
  - brak anonimowości przy prostych realizacjach (np. numer IP nadawcy)

Inne problemy

- Wysyłanie głosów pocztą
  - czy kupowanie głosów, nierealne?
    - USA, NJ 2004, senator Jon Corzine wydał 65$ mln na kampanię, otrzymał 1.470 tys. głosów, co daje 44$ na głos.
    - Niemcy 2002, można było kupić paczkę 10.000 głosów za 59.000 EUR,
  - niszczenie głosów z określonych regionów (Broward County, Floryda, 2000 - 58.000 głosów zniknęło z urzędu pocztowego - hrabstwo z wyraźną przewagą Gore'a)
- Głosowanie przez internet
  - łatwość sprzedawania/kupowania głosów
  - brak anonimowości przy prostych realizacjach (np. numer IP nadawcy)
  - ataki hackerskie (np. atak na serwery DNS)

Co to jest e-voting?

- e-voting = głosowanie przy pomocy maszyn elektronicznych

Co to jest e-voting?

- e-voting $=$ głosowanie przy pomocy maszyn elektronicznych
- e-voting $\neq$ wybory przez internet

Co to jest e-voting?

- e-voting $=$ głosowanie przy pomocy maszyn elektronicznych
- e-voting $\neq$ wybory przez internet
- maszyna do głosowania to
  - specjalne dedykowane urządzenia (drogo!),
  - albo komputer + drukarka (wykorzystanie istniejącej infrastruktury publicznej - taniej, niekoniecznie mniej bezpieczne)

Wymagania wobec e-voitingu

- anonimowość głosujących,

Wymagania wobec e-voitingu

- anonimowość głosujących,
- głosujący powinien móc sprawdzić, że jego głos został policzony,

Wymagania wobec e-voitingu

- anonimowość głosujących,
- głosujący powinien móc sprawdzić, że jego głos został policzony,
- głosujący nie może mieć możliwości sprzedaży głosu (ani udowodnić jak głosował),

Wymagania wobec e-voitingu

- anonimowość głosujących,
- głosujący powinien móc sprawdzić, że jego głos został policzony,
- głosujący nie może mieć możliwości sprzedaży głosu (ani udowodnić jak głosował),
- oddany głos nie może być zmieniony ani usunięty z systemu,

Wymagania wobec e-voitingu

- anonimowość głosujących,
- głosujący powinien móc sprawdzić, że jego głos został policzony,
- głosujący nie może mieć możliwości sprzedaży głosu (ani udowodnić jak głosował),
- oddany głos nie może być zmieniony ani usunięty z systemu,
- nie można bezkarnie dorzucić głosów do urny,

Wymagania wobec e-voitingu

- anonimowość głosujących,
- głosujący powinien móc sprawdzić, że jego głos został policzony,
- głosujący nie może mieć możliwości sprzedaży głosu (ani udowodnić jak głosował),
- oddany głos nie może być zmieniony ani usunięty z systemu,
- nie można bezkarnie dorzucić głosów do urny,
- system musi być zrozumiały dla przeciętnego wyborcy

Obecnie stosowane maszyny głosujące w USA

"... bez komentarza..."

Rozwiązania – system Davida Chauma

- spełnia wszystkie wymagania, ale...

Rozwiązania – system Davida Chauma

- spełnia wszystkie wymagania, ale...
- jest drogi - wymaga specjalnych drukarek (drukowanie dwustronne na plastikowych kartach),
- jego zrozumienie wymaga dużej wprawy matematycznej

Wrocławski E-voting

Głosujący w kabinie do głosowania- etap 1

- maszyna przygotowuje wirtualną kartę do głosowania,

Głosujący w kabinie do głosowania- etap 1

- maszyna przygotowuje wirtualną kartę do głosowania,
- głosujący otrzymuje kontrolny wydruk z kodami (*zastosowane funkcje hashujące*):
  - maszyna nie może już zmienić karty.

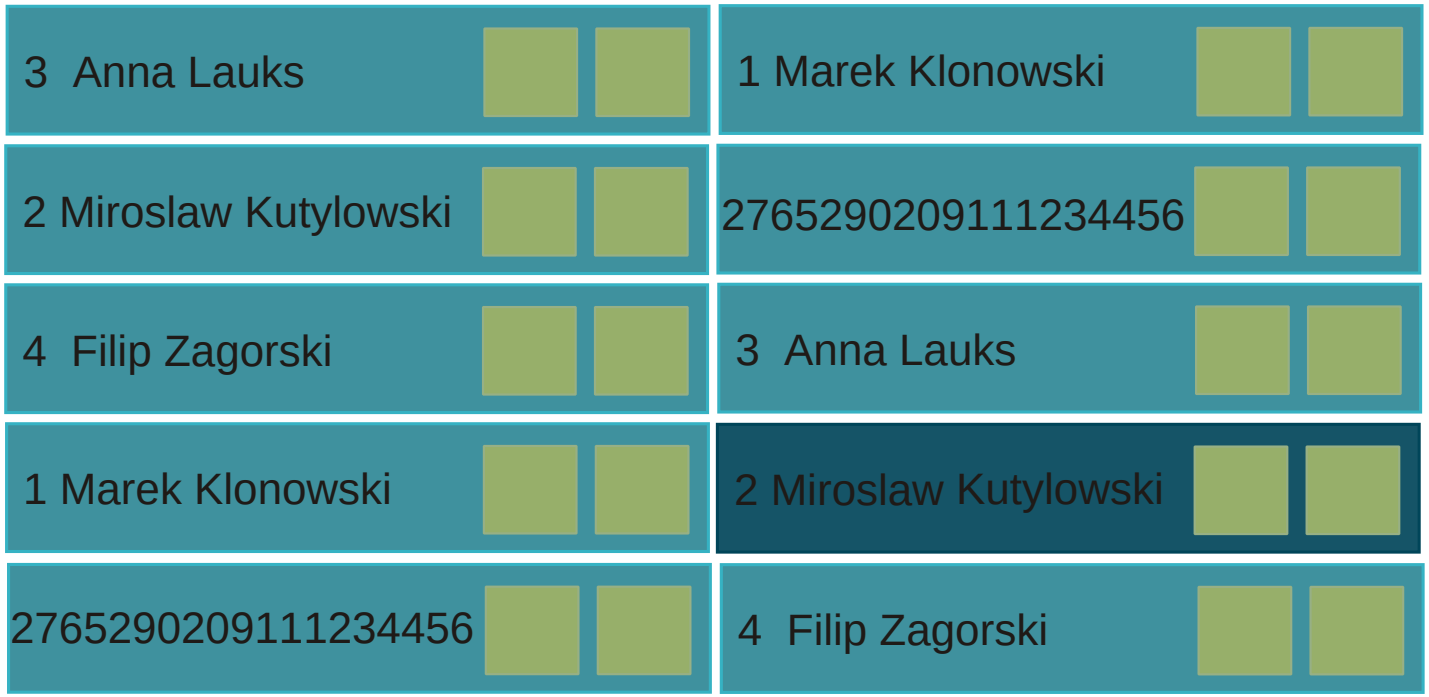
Głosujący w kabinie do głosowania - etap 2

- głosujący widzi na ekranie:

3 Anna Lauks	1 Marek Klonowski
2 Miroslaw Kutylowski	276529020911234456
4 Filip Zagorski	3 Anna Lauks
1 Marek Klonowski	2 Miroslaw Kutylowski
276529020911234456	4 Filip Zagorski

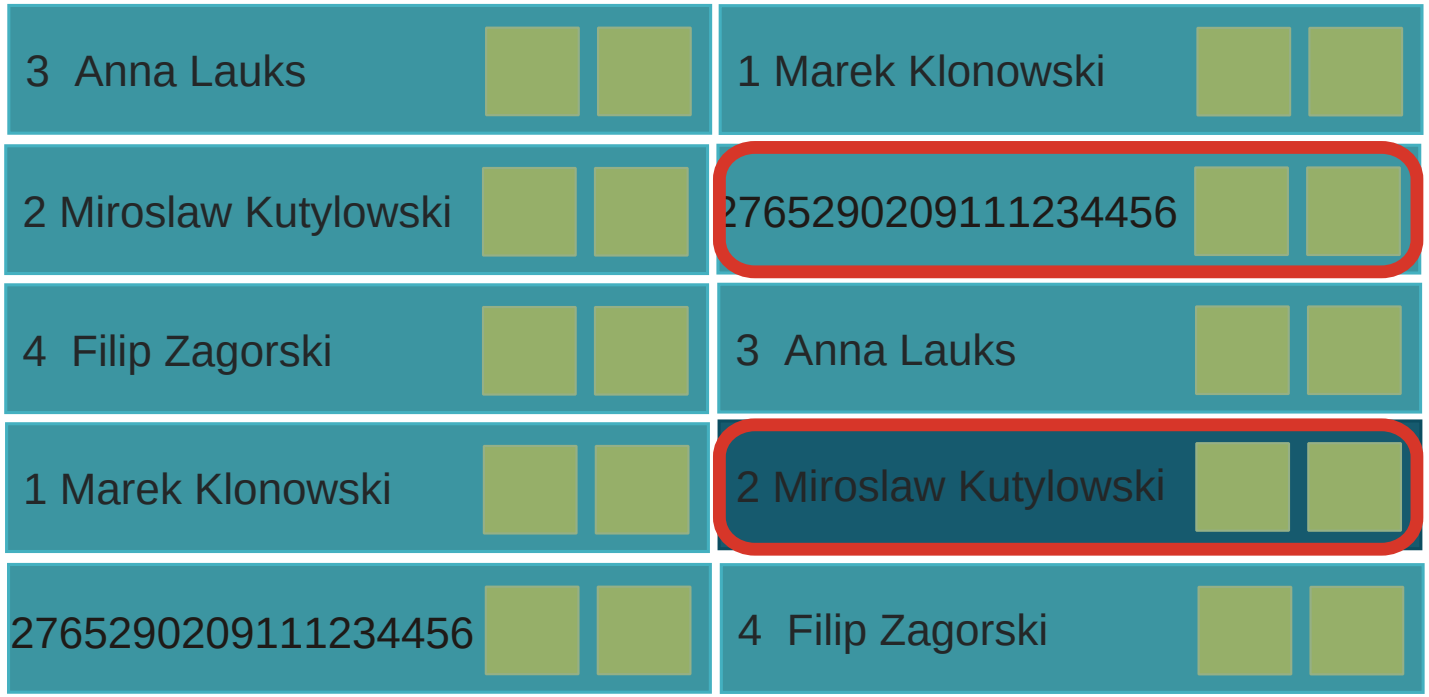
Głosujący w kabinie do głosowania - etap 2

- Głosujący wybiera kandydata (w jednej z dwóch kolumn):



Głosujący w kabinie do głosowania - etap 2

- Głosujący wybiera kandydata (w jednej z dwóch kolumn):

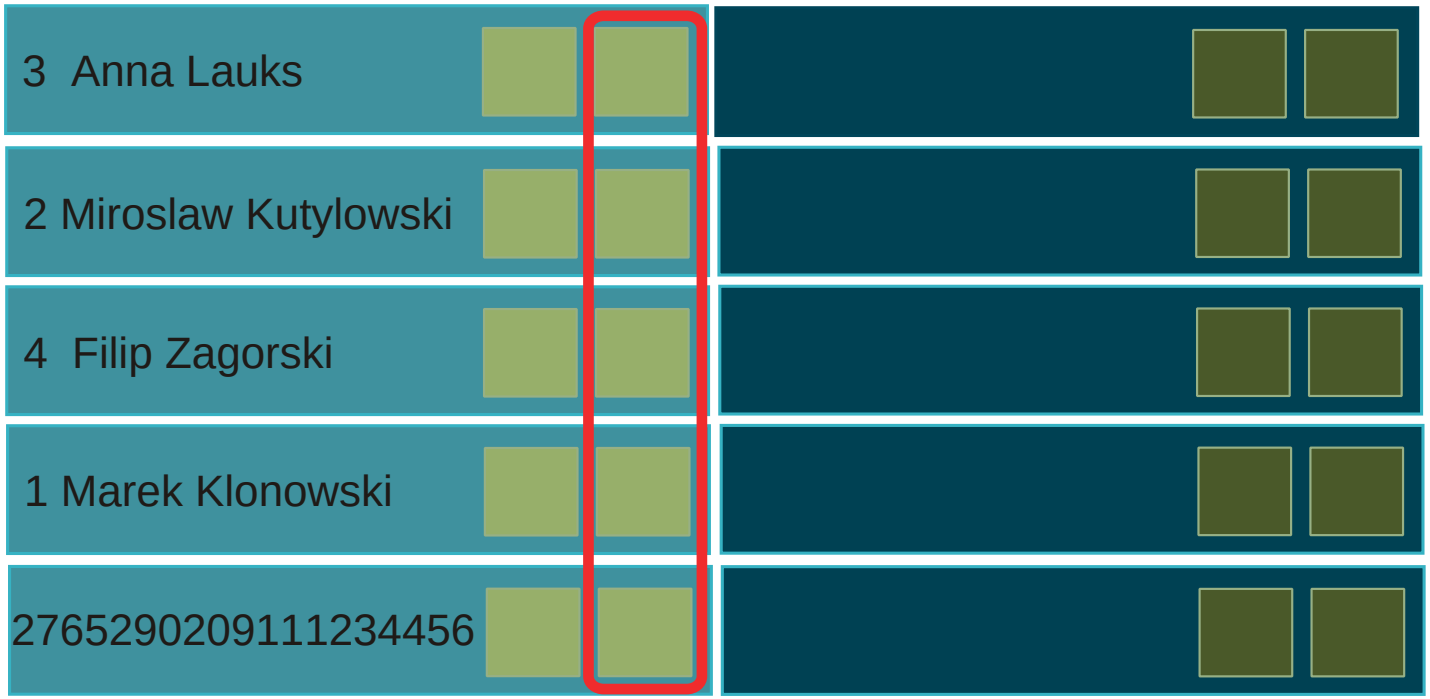


Głosujący w kabinie do głosowania - etap 3

- głosujący dostaje wydruk - zaszyfrowany głos:

Głosujący w kabinie do głosowania - etap 4

- przygotowanie wydruku kontrolnego:



Głosujący w kabinie do głosowania - etap 5

- głosujący otrzymuje drugi wydruk kontrolny:

Karta do weryfikacji

3 Anna Lauks	Reiopenl92nhdvampsddkffp
2 Miroslaw Kutylowski	Wqwje91nbe43mipwugfhiu
4 Filip Zagorski	Jobwjb821q10nxnimmajwax
1 Marek Klonowski	Pquioeiuwdf7218nzoiqpjq11
27652902091112344 56	Oqihiqhrt098hk2229kPiuo

Skanowanie zakodowanych głosów

- w obecności głosującego komisja skanuje zakodowany głos,
- wydruki ostemplowane przez Komisję - dowód do ewentualnych reklamacji.

Zliczanie głosów

Zeskanowane kody są

- przetwarzane kryptograficznie,
- mieszane losowo

kolejno przez różne Komisje (Serwery) Skrutacyjne.

- gwarancja anonimowości
- **połówki rozdzielane!**

Zliczanie głosów

- Ostatnia komisja otrzymuje i publikuje odszyfrowane głosy i identyfikatory:
  - pasujące pary identyfikatorów,
  - pasujące pary głosów.

Zliczanie głosów

- Ostatnia komisja otrzymuje i publikuje odszyfrowane głosy i identyfikatory:
  - pasujące pary identyfikatorów,
  - pasujące pary głosów.
- Głosujący może sprawdzić, czy jego para identyfikatorów jest na liście.

Dlaczego maszyna głosująca nie może oszukiwać

Maszyna głosująca:

- nie podłączona do sieci - nie może komunikować się,
- nie może zmienić raz przygotowanej karty do głosowania,
- głosujący może sprawdzić zawartość połówki wybranej do weryfikacji - procedura kryptograficzna dla 2 karty kontrolnej.

Niemożność manipulacji

- zakodowane głosy i identyfikatory są nierozróżnialne,
- nie widać gdzie są pasujące połówki.

Niemożność manipulacji

- zakodowane głosy i identyfikatory są nierozróżnialne,
- nie widać gdzie są pasujące połówki.

Próby manipulacji:

- usunięcie głosu - uda się jedynie, gdy trafimy na obie jego połówki
  przy 1000 głosujących prawdopodobieństwo $1/8000$,
  dla 4 głosów: szansa mniej niż 1 do biliona,
- gdy przypadkiem usuniemy choćby połówkę identyfikatora - wyda się,
- kryptograficzna procedura pozwala ustalić, która komisja skrutacyjna dokonała manipulacji.

Dlaczego wyborca nie może oszukać?

- na kartach do weryfikacji ma jedynie połówki!
  nie może ich użyć jako dodatkowego głosu

Podsumowanie cech

- prosty, standardowy hardware,
- **niemożność** fałszowania wyborów,
- **wyborca** może przekonać się, że jego głos liczony,
- redukcja kosztów, prosta logistyka, dokładność wyników.

pilotażowa implementacja realizowana na PWr

Dziękujemy za uwagę!