System głosowania elektronicznego

Autor:
Michał Rajkowski
Opiekun:
prof. dr hab. inż. Zbigniew Kotulski

Spis treści

Wprowadzenie

- Systemy głosowania elektronicznego (ang. electronic voting systems)
- Coraz większa cyfryzacja społeczeństwa -> cyfryzacja wyborów

- **Wygoda** – możliwość głosowania np. przez Internet
- **Wydajność** – znacznie skrócony czas potrzebny na obliczanie wyniku wyborów

Wprowadzenie

- **Dokładność** – dużo większa niż w przypadku ręcznego liczenia głosów
- **Koszt** – znaczne oszczędności na „fizycznych” elementach systemu
- **Dodatkowe zalety**– znacznie skrócony czas potrzebny na obliczanie wyniku wyborów

Klasyfikacja

- Systemy głosowania elektronicznego można klasyfikować pod dwoma względami:

1) Stopień wirtualizacji
2) Uzyskane cechy bezpieczeństwa

Klasyfikacja

- Stopień wirtualizacji oznacza jak bardzo dany system odchodzi od oryginalnej (fizycznej) formy a zmierza w kierunku wyborów całkowicie wirtualnych

1) **Elektroniczna wirtualizacja wyników głosowania**
   a) Systemy komputerowe spełniają jedynie rolę pomocniczą przy zbieraniu i wizualizacji wyników wyborów
   b) Proces głosowania oraz liczenia głosów pozostaje niezmienny
   c) Z racji roli ogrywanej przez system, wymagania bezpieczeństwa są niskie

Klasyfikacja

2) **Głosowanie wspomagane elektronicznie**
   a) Systemy komputerowe obsługują przyjmowanie i zliczanie głosów
   b) Wyborcy oddają głosy w lokalach wyborczych na specjalnych terminalach (ang. voting machines)
   c) Pozwala na stopniową wirtualizację procesu wyborów
   d) Wymagania bezpieczeństwa są dużo wyższe niż w poprzednim przypadku

Klasyfikacja

3) **Głosowanie zdalne**
   a) Głosy oddaje się zdalnie z dowolnej lokalizacji za pomocą medium, które taką wymianę danych umożliwia (np. Internet, sieć GSM)
   b) Obsługą wyborów zajmują się odpowiednie serwery centralne
   c) Oznacza to pełną wirtualizację procesu wyborów oraz najwyższe wymagania bezpieczeństwa
   d) Bardzo ważne jest odpowiednie rozwiązanie problemu identyfikacji wyborców (np. podpis kwalifikowany)

Klasyfikacja

- Cechy bezpieczeństwa pozwalają określić jak bezpieczny jest dany system głosowania oraz czy spełnia określone przez nas wymagania.

1) **Privacy** (prywatność)– relacja głosująca–oddany głos musi pozostać tajemnicą, tak by wyborcy mogli wyrażać swoją wolę bez obawy o bycie zastraszonym
2) **Accuracy** (dokładność)– wyniki wyborów muszą dokładnie odzwierciedlać wybór dokonany przez głosujących
3) **Receipt-freeness** (brak pokwitowania) – oznacza brak możliwości, by głosujący był w stanie uzyskać/stworzyć ‘paragon’, który potwierdzałby w jaki sposób głos został oddany; cecha ta ma na celu zapobieganie sprzedaży/kupnie głosów
4) **Eligibility** (kwalifikowalność)– tylko głosujący posiadający prawa wyborcze mogą głosować, wszystkie głosy oddane przez osoby nie uprawnione nie są brane pod uwagę
5) **Un-reusability** (brak reutylizacji) – każda uprawniona do głosowania osoba może oddać tylko jeden poprawny głos, tak by każdy wyborca posiadał jednakowy (cząstkowy) wpływ na końcowy wynik wyborów

Klasyfikacja

6) **Fairness** (uczciwość) – żadne częściowe wyniki nie są prezentowane przed oficjalnym zakończeniem wyborów, tak by dochować całkowitej prywatności wyborów oraz dać wszystkim kandydatom równe szanse
7) **Robustness** (rzetelność) – system pozostaje bezpieczny nawet wtedy, gdy występują pewne zakłócenia/awarię (oczywiście tylko do pewnego stopnia), niezależnie od ich źródła (głosujący, administracja, czy czynniki zewnętrzne)
8) **Completeness** (całkowitość) – wszystkie poprawnie oddane głosy muszą zostać poprawnie zliczone
9) **Soundness** (solidność) – odporność na błędy/zakłócenia – przykładem może być zabezpieczenie system by nieuczciwy głosujący nie mógł przerwać procesu głosowania
10) **Inalterability** (nienaruszalność) – po oddaniu głosu przez głosującego nie ma możliwość jego zmiany ani przez głosującego, ani przez nikogo innego (zarówno z jak i spoza systemu)

Klasyfikacja

11) **Personal verifiability** (osobista weryfikowalność)– musi istnieć możliwość sprawdzenia czy wynik głosowania jest poprawny i czy ktoś niepowołany nie wpłynął na niego podczas trwania wyborów; wyborca musi mieć możliwość sprawdzenia czy jego głos został poprawnie oddany
12) **Universal verifiability** (powszechna weryfikowalność) – podobnie jak w przypadku wyżej, z tą różnicą, że każdy ma możliwość sprawdzenia poprawności wyborów
13) **Dispute-freeness** (bezsporność) – fakt, że uczestnicy głosowania (głosujący/administracja) postępują zgodnie z protokołem głosowania może być publicznie potwierdzony (w dowolnej fazie wyborów) przez dowolną osobę (z i spoza systemu)
14) **Incoercibilty** (nieprzymuszalność) – nie może istnieć możliwość zmuszenia do oddawania głosu wbrew ich woli czy przekonaniu

Aplikacja – Założenia

- Celem pracy jest stworzenie prostego systemu głosowania elektronicznego
- Musi spełniać podstawowe wymagania bezpieczeństwa
- Musi być stosunkowo prosty w implementacji

Aplikacja – Założenia

- Zaprojektowany schemat opiera się w głównej mierze na:

1) Ślepym podpisie (ang. blind signature)
2) Zaślepianiu bitowym XOR
3) Certyfikatach

- Dzięki temu uzyskujemy system, który pozwala na implementację wymaganych cech bezpieczeństwa przy stosunkowo prostej implementacji

Aplikacja – Protokoły i algorytmy

1) **Diffie-Hellman –** jest to protokół kryptograficzny, który pozwala w bezpieczny sposób ustalić dwóm stronom wspólny sekret. Dodatkowo, otrzymanie tego sekretu na podstawie treści wymienionych wiadomości między stronami jest praktycznie niemożliwe. Sekret ten jest później używany do ustalenia wspólnego klucza sesyjnego, używanego do szyfrowania komunikacji.

2) **AES (Advanced Encryption Standard) –** to symetryczny szyfr blokowy; W naszym systemie AES jest używany do szyfrowania wiadomości przesyłanych między poszczególnymi elementami systemu. Główną zaletą AES jest szybkość działania (w porównaniu do wydajności kryptograficznej szyfru RSA) oraz stosunkowo wysokie bezpieczeństwo – nawet klucz 128 bitowy jest już bardzo trudny do złamania.

Aplikacja – Protokoły i algorytmy

3) **RSA (Rivest–Shamir–Adleman)** – Jest to jeden z pierwszych i obecnie jeden z najpopularniejszych asymetrycznych algorytmów kryptograficznych. Można go stosować zarówno do szyfrowania jak i do podpisów cyfrowych. Bezpieczeństwo szyfrowania opiera się na trudności faktoryzacji dużych liczb złożonych.

4) **Blind Signature (Ślepy podpis)** Protokół ślepych podpisów jest w kryptografii formą cyfrowego podpisu, w którym podpisywany dokument nie jest znany osobie podpisującej. Ślepy podpis może być potem zweryfikowany z wiadomością. Ślepe podpisy są na ogół wykorzystywane w protokołach opartych na prywatności, w których autor wiadomości i podpisujący to różne osoby.

Aplikacja – Protokoły i algorytmy

Ślepy podpis oparty na RSA:

- A zaślepia wiadomość m

$$m' \equiv mr^e \pmod{N}$$

- B tworzy s' (podpis zaślepionej wiadomości m')

$$s' \equiv (m')^d \pmod{N}.$$

- A odślepia s' i uzyskuje s (podpis wiadomości m)

$$s \equiv s' \cdot r^{-1} \pmod{N}$$

- Dowód na poprawność

$$s \equiv s' \cdot r^{-1} \equiv (m')^d r^{-1} \equiv m^d r^{ed} r^{-1} \equiv m^d r r^{-1} \equiv m^d \pmod{N}$$

Aplikacja – schemat działania

1) UC generuje certyfikat cyfrowy dla każdego zarejestrowanego wyborcy
2) Każdy z wyborców używa uzyskanego certyfikatu do uzyskania od KW losowej sekwencji bitowej B_i (karta wyborcza)
3) Każdy wyborca konstruuje swój głos v_i
   a) Jeżeli głos jest oddanych na pierwszą opcję to:
      $v_i = B_i \oplus (0,\ldots,0,\ 1\ ,0,\ldots,0)$ 1 na i-tym miejscu
   b) Jeżeli głos jest oddanych na drugą opcję to:
      $v_i = B_i \oplus (0,\ldots,0)$
4) Każdy wyborca wybiera sekwencję losową C_i i oblicza

$$P_i = v_i \oplus C_i$$

Aplikacja – schemat działania

5) Wyborca tworzy P_i^* i przesyła ją do UC
6) UC podpisuje P_i^* i zwraca $S(P_i)^*$ do wyborcy
7) Wyborca usuwa zaślepienie i wysyła $S(P_i)$ do CKW
8) Wyborca wysyła C_i do UC
9) UC oblicza C i wysyła je do CKW

$$C=C_1 \oplus C_2 \oplus \ldots \oplus C_n$$

10) KW oblicza B i wysyła je do CKW

$$B=B_1 \oplus B_2 \oplus \ldots \oplus B_n$$

11) CKW sprawdza podpisy $S(P_1)\ldots S(P_n)$ i uzyskuje $P_1\ldots P_n$

Aplikacja – schemat działania

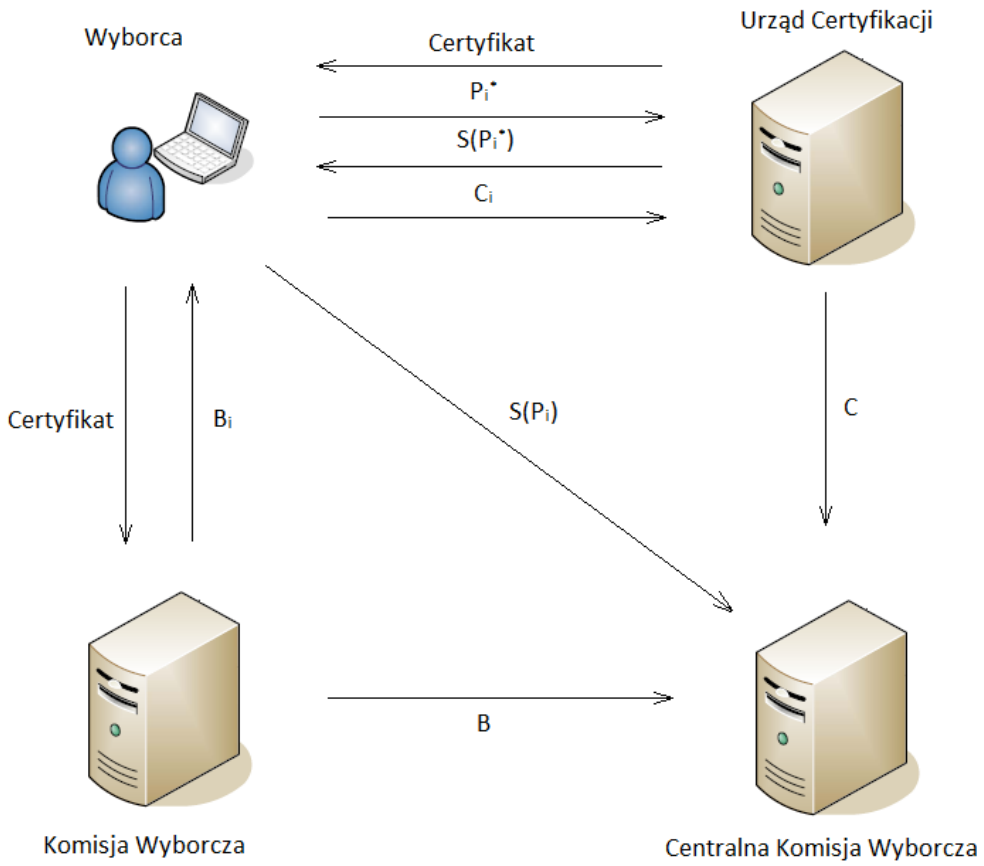
12) CKW oblicza

$$P = P_1 \oplus P_2 \oplus \ldots \oplus P_n$$

$$v = P \oplus C = v_1 \oplus v_2 \oplus \ldots \oplus v_n$$

13) CKW oblicza liczbę głosów na opcję nr 1 i 2 za pomocą odległości Hamminga
    a) Liczba głosów na opcję nr 1:
       odległośćHamminga(v,B)
    b) Liczba głosów na opcję nr 2:
       N-odległośćHamminga(v,B)
14) CKW publikuje $P_1 \ldots P_n$ oraz **C**

Aplikacja – Architektura



Aplikacja – Uzyskane cechy

1) **Prywatność**
   - Dzięki zastosowaniu ślepego podpisu oraz zaślepień bitowych
   - UC zna tylko C_i co nie wystarcza do obliczenia v_i, nie znając B_i.
   - KW zna tylko B_i, co również nie wystarcza do odgadnięcia v_i.
   - CKW zna P_i, ale nie zna ani B_i, ani C_i, gdyż posiada jedynie sumy XOR C i B.
2) **Kwalifikowalność**
   - Urząd Certyfikacji, wystawia certyfikaty potwierdzające tożsamość
   - Do wyborów mogą przystąpić jedynie uprawnieni wyborcy (zarejestrowani w bazie danych AC)

Aplikacja – Uzyskane cechy

3) **Weryfikowalność**
   - Każdy wyborca zna swoje Pi, a po zakończeniu wyborów CKW publikuje C oraz listę wszystkich P_x użytych do obliczenia wyniku końcowego.
   - Dzięki temu istnieje możliwość sprawdzenia czy nasz głos został uwzględniony przy obliczaniu wyniku wyborów.
4) **Uczciwość**
   - Sama konstrukcja system nie pozwala na publikowanie wyników pośrednich
   - Można opublikować jedynie wyniki końcowe

Aplikacja – Uzyskane cechy

5) **Wyjątkowość**
   - Głos wyborcy zajmuje określone miejsce w ciągu bitowym
   - Bit przyjmuje jedynie wartość 1 lub 0
   - Sama konstrukcja protokołu głosowania uniemożliwia oddanie wyborcy więcej niż jednego głosu
6) **Całkowitość**
   - Każdy poprawny głos jest podpisywany (ślepym podpisem) przez UC
   - CKW, która zna klucz publiczny AC, może sprawdzić poprawność każdego głosu
   - Każdy poprawny głos jest uwzględniany przy wyliczaniu końcowego wyniku.

Podsumowanie

- System spełnia najważniejsze cechy bezpieczeństwa
- Jest łatwy w implementacji
- Pozwala na bardzo „lekkie” rozwiązanie problemu prywatności

Literatura

1. A Critical Review of Receit-Freeness and Coercion-Resistance, Bo Meng, School of Computer, South-Center Univeristy for Nationalities, Hubei, 2009
2. Design and analysis of a practical e-voting protocol, Marian Novotny, Institute of Computer Science, Pavol Jozef Safarik University, 2009
3. The Theory and Implementation of an Electronic Voting System, Ivan Damgard, Jens Groth and Gorm Salomonsen, 2003
4. Implementation Issues In Secure E-Voting Schemes Riza Aditya, Byoungcheon Lee, Colin Boyd and Ed Dawson, Information Security Research Centre, Queensland University of Technology, 2008
5. Analysis of an Electronic Voting System, Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, Dan S. Wallach, 2007
6. Security Considerations for Remote Electronic Voting over the Internet, Avi Rubin, AT&T Labs – Research, 2009

Dziękuję za uwagę