ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2013
Seria: ORGANIZACJA I ZARZĄDZANIE z. 64 Nr kol. 1894

Marcin SOBOTA
Politechnika Śląska
Instytut Ekonomii i Informatyki

KWANTOWE KARTY DO GŁOSOWANIA

Streszczenie. Artykuł przedstawia model głosowania elektronicznego wykorzystującego kwantowe karty do głosowania opierające się na protokołach kwantowego uzgadniania klucza. Silną stroną modelu jest wykorzystanie zabezpieczeń opartych na prawach fizyki w miejsce bezpieczeństwa obliczeniowego.

QUANTUM VOTING CARDS AS AN ALTERNATIVE FOR CLASSIC ALGORITHMS OF PUBLIC KEY DISTRIBUTION.

Summary. The article presents the model using quantum e-voting cards based on protocols of quantum key distribution. The strength of the model is using security based on the laws of physics in a place of computing security.

1. Wstęp

Oddanie głosu drogą elektroniczną, w wyborach parlamentarnych czy prezydenckich nie jest niczym nowym. W wielu krajach obywatele maja taką możliwość. Głosowanie elektroniczne jest jednak jedynie dodatkiem do wyborów realizowanych metodami tradycyjnymi. W dobie elektronicznego rozwoju może okazać się, że oddanie głosu drogą elektroniczną będzie jedyną z możliwych. Aby to się jednak stało należy zbudować modele głosowania, które w sposób wystarczający zapewnią bezpieczeństwo na każdym z etapów prowadzących do ogłoszenia wyników wyborów.

2. Bezpieczeństwo głosowania elektronicznego – kryptografia klasyczna

Bezpieczeństwo danych transmitowanych drogą elektroniczną zapewniane jest poprzez wykorzystanie metod kryptografii klasycznej w tym:

- Prostych metod uwierzytelniania użytkownika,
- Podpisu cyfrowy,
- Kryptograficznych algorytmów asymetrycznych,
- Kryptograficznych algorytmów symetrycznych.

Mechanizmy zapewniające należyty poziom uwierzytelniania [1] użytkownika zawarte są w dokumentacji ISO/IEC w tym szczegółowo w dokumentach ISO/IEC 9796 (mechanizm schematu podpisu cyfrowego), ISO/IEC 9797 (kod uwierzytelniania wiadomości), ISO/IEC 9798 (mechanizmy uwierzytelniania podmiotów stosujących symetryczne algorytmy szyfrowania, metody z kluczem publicznym, kryptograficzną funkcję kontrolną) oraz kilku innych dokumentach Międzynarodowej Organizacji Normalizacyjnej (ISO) oraz Międzynarodowej Komisji Elektrotechnicznej (IEC). Opis kryptograficznych algorytmów symetrycznych i asymetrycznych znaleźć można między innymi w [1], [2], [3], [4], [6], [7].

Wszystkie wspomniane mechanizmy wykorzystywane są w realizowanych protokołach głosowania elektronicznego z których wybrany przedstawiony jest poniżej:

1. Każdy uprawniony wyborca otrzymuje od Głównej Agencji Uprawnień (GAU) numer rejestracyjny. Dodatkowo GAU przechowuje wszystkie wydane numery celem późniejszego sprawdzenia czy dana osoba nie próbuje głosować drugi raz.
2. GAU przesyła numery rejestracyjne do GKW (Głowna Komisja Wyborcza).
3. Wyborca swój głos wraz z nadanym numerem rejestracyjnym szyfruje kluczem publicznym GKW.
4. GKW deszyfruje głos swoim kluczem prywatnym. Następnie sprawdza czy numer identyfikacyjny znajduje się na liście otrzymanej od GAU. Jeśli numeru tam nie ma głos zostaje odrzucony, jeśli jest, głos zostaje dodany oraz numer identyfikacyjny zostaje usunięty z listy.
5. Po odebraniu wszystkich głosów GKW ogłasza wyniki wyborów, publikuje listę numerów identyfikacyjnych oraz na kogo ich właściciele głosowali.

Przedstawiony protokół zawiera wszystkie z czterech wspomnianych mechanizmów zabezpieczeń:

1. Proste uwierzytelnianie pojawia się w momencie odbioru numeru identyfikacyjnego od GAU – poświadczeniem jest przedstawiony dowód tożsamości.
2. Podpis cyfrowy w postaci wykorzystanego klucza prywatnego osoby głosującej.
3. Klasyczne algorytmy symetryczne i asymetryczne w postaci podpisu osoby głosującej oraz szyfrogramu wykorzystującego klucz symetryczny oraz publiczny klucz GKW.

3. Protokół kwantowego uzgadniania klucza kryptograficznego

Protokołem, którego zmodyfikowana wersja ma zostać wykorzystana do realizacji kwantowych kart do głosowania jest protokół BB84. Z założenia protokół służy do uzgadniania kryptograficznego klucza symetrycznego z wykorzystaniem polaryzacji światła. Autorami protokołu są: Charles Bennett, Gilles Brassard i Artur Ekert. Opiera się on na zastosowaniu dwóch alfabetów:

- prostego zawierającego fotony o polaryzacji 0^o i 90^o (odpowiednio binarne 0 i 1),
- ukośnego zawierającego fotony o polaryzacji 45^o i 135^o (odpowiednio binarne 0 i 1).

Kolejne jego kroki wyglądają następująco:

1) Alicja (nadawca) wybiera losowo jedną z czterech możliwych polaryzacji i wysyła do Bolka (odbiorca) foton o takiej polaryzacji. Ciąg fotonów stanowi ciąg zer i jedynek z dwóch alfabetów kwantowych.
2) Bolek wybiera losowo bazę prostą lub ukośną i wykonuje pomiar polaryzacji każdego fotonu, który otrzymał od Alicji.
3) Bolek notuje wyniki pomiaru zachowując je w tajemnicy.
4) Bolek publicznie informuje Alicję, jakich baz użył do pomiaru, zaś Alicja informuje go czy wybrane losowo typy baz były właściwe czy nie.

Alicja i Bolek przechowują wyniki pomiarów, dla których Bolek użył właściwej bazy. Wyniki tych pomiarów można zapisać w postaci binarnej a uzyskany ciąg może zostać wykorzystany jako klucz kryptograficzny.

Szczegóły dotyczace protokołu można znaleźć w [5].

4. Model głosowania elektronicznego z wykorzystaniem metod kwantowych

Jak wspomniano w poprzednim rozdziale model głosowania elektronicznego z wykorzystaniem metod kwantowych opierał się będzie na zmodyfikowanym protokole BB84. W protokole BB84 generowany jest losowy ciąg bitów kodowanych za pomocą polaryzacji światła na który strona odbierająca nakłada losowo wybrane bazy dokonując odczytu polaryzacji. W przypadku głosowania elektronicznego nadawca wiadomości (GKW) starannie przygotowuje polaryzacje poszczególnych fotonów (nie jest to ciąg losowy) w taki sposób by odpowiadały one ciągowi przypisanemu konkretnej karcie do głosowania.

Jeśli np. karta do głosowania nr 25 jest zakodowana jako ciąg 50-cio bitowy:

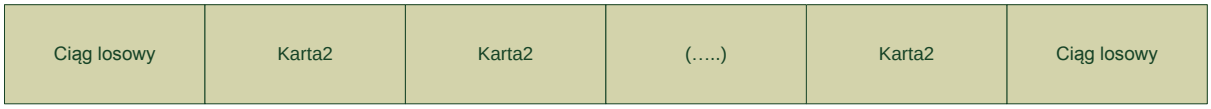
10010100100101001010010010001001010110100101010

to nadawca (GKW) musi tak przygotować polaryzacje poszczególnych fotonów, aby w wykorzystywanych bazach odpowiadały one wartościom 0 i 1. GKW musi wykonać jeszcze jedno działania. Oprócz przypisania karcie do głosowania pewnego ciągu bitów, który musi być znany głosującemu, GKW musi utworzyć te listy w taki sposób, by głosujący wiedział na kogo oddaje głos. Przykład ciągów przypisanych karcie przedstawia rysunek 1 natomiast wygląd kart do głosowania prezentuje rysunek 2.

Rys. 1. Przykład ciągów bitów przypisanych kartom do głosowania
Fig. 1. Example of bit strings assigned to vote cards

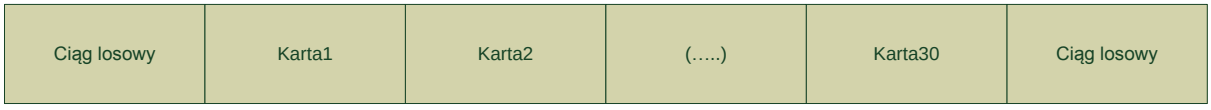
Rys. 2. Przykład kart do głosowania
Fig. 2. Example of voting cards

W momencie kiedy głosujący chce oddać głos łączy się ze stroną GKW, zostaje uwierzytelniony i rozpoczyna się proces uzgadniania karty do głosowania. GKW wysyła ciąg bitów zakodowanych za pomocą polaryzacji światła który może wyglądać jak na rysunku 3.



Rys. 3. Przykładowy ciąg wysłany przez GKW
Fig. 3. Example of string sent by GKW

Na tak przygotowany ciąg bitów przez GKW głosujący nakłada starannie przygotowany ciąg baz dzięki którym może dokonać odczytu poszczególnych polaryzacji. Przedstawia to rysunek 4.



Rys. 4. Bazy odpowiadające poszczególnym kartom nakładane przez głosującego
Fig. 4. Bases corresponding to different cards imposed by voting

Złożenie ciągu bitów wysłanych przez GKW oraz baz nakładanych przez głosującego wygląda jak na rysunku 5.

Ciąg losowy	Karta2	Karta2	(…..)	Karta2	Ciąg losowy
Ciąg losowy	Karta1	Karta2	(…..)	Karta30	Ciąg losowy

Rys. 5. Przykład uzgadniania karty do głosowania
Fig. 5. Example of ballot reconciliation

GKW przygotowuje tyle kart do głosowania ilu jest kandydatów, zmieniając na każdej karcie kolejność kandydatów, tak by prawdopodobieństwo wystąpienia kandydata na każdej pozycji było równe dla wszystkich kart. Następnie GKW wysyła do uprawnionego do głosowania wybraną losowo kartę (ciąg bitów który jej odpowiada) w układzie przedstawionym na rys. 5. Ciągi losowe na początku i końcu stanowią dokładne odzwierciedlenie działania protokołu BB84 i ich celem jest wyłapanie ewentualnego podsłuchu występującego na łączu. Ciąg bitów odpowiadający wybranej przez GKW karcie do głosowania jest powtarzany tyle razy ile jest różnych kart do głosowania. Głosujący nakłada bazy pozwalające prawidłowo odczytać kolejno kartę nr 1, kartę nr 2, kartę nr 3 itd. Kiedy wybór jest nieprawidłowy, np. dla wysłanej przez GKW karty nr 2 głosujący wybrał bazy dla karty nr 1 otrzyma wyniki które nie będą odpowiadały żadnej ze znanych mu kombinacji bitów (nie rozpozna karty), natomiast przy odpowiednim doborze baz rozpozna kartę. Układ ten prezentuje rys. 6

Ciąg losowy	Karta2	Karta2	(…..)	Karta2	Ciąg losowy
Ciąg losowy	Karta1	Karta2	(…..)	Karta30	Ciąg losowy
Sprawdzenie podsłuchu	Błąd	Karta rozpoznana	(…..)	Błąd	Sprawdzenie podsłuchu

Rys. 6. Schemat uzgadniania karty do głosowania
Fig. 6. Schematic ballot reconciliation

Kiedy głosujący rozpozna kartę przygotowaną przez GKW wystarczy jedynie że zaznaczy preferowanego przez siebie kandydata i wyśle stosowną informację do GKW. Mocną stroną tego modelu jest to, że głos może zostać wysłany kanałem otwartym i nikt nie jest w stanie określi na kogo został oddany głos. Oczywiście, tematem odrębnym jest zachowanie integralności przesłanych danych dotyczących wybranego kandydata ale można ten problem rozwiązać prostym mechanizmem potwierdzającym wybór kandydata (GKW wysyła informację zwrotną do głosującego).

5. Podsumowanie i wnioski

Silną stroną prezentowanego modelu jest zastosowanie protokołu kwantowego gwarantującego bezpieczeństwo dzięki prawom fizyki. Zgodnie z zasadą nieoznaczoności Heisenberga nie można dokonać pomiarów w dwóch bazach jednocześnie co oznacza, że akt pomiaru zawsze wprowadza zakłócenia, które wskazują na wystąpienie podsłuchu. Dodatkowo istotnym elementem modelu jest całkowita przejrzystość oddanego głosu (nie wiedząc która karta została wykorzystana podsłuchujący nie wie który z kandydatów został wybrany). Słabość przedstawionego modelu wynika z konieczności zastosowania odpowiedniego sprzętu realizującego protokoły kwantowe, który w chwili obecnej jest trudno dostępny i bardzo drogi. Jednak zważywszy na stały postęp w dziedzinie mechaniki i fizyki kwantowej można przypuszczać, że w niedalekiej przyszłości sprzęt ten stanie się dostępny za rozsądne pieniądze.

Bibliografia

1. Menezes, A.J., van Oorschot, P.C., Vanstone, S.A. *Handbook of Applied Cryptography.* New York CRC Press, 1997.
2. Schneier, B. *Kryptografia dla praktyków.* Warszawa PWN, 2001.
3. Simmons, G. *Symmetric and Asymmetric Encryption.* New York ACM Computing Surveys, 1979.
4. Stinson, D.R. *Kryptografia w teorii i w praktyce.* Warszawa Wydawnictwo Naukowo-Techniczne, 2005.
5. Bennett, Charles i Brasard, Gilles. *Quantum Cryptography: Public key distribution and coin tossing.* brak miejsca : Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, 1984.
6. Karbowski, M. *Podstawy kryptografii.* Gliwice Helion, 2008.
7. Klamka J., Węgrzyn S., Bugajski S.: ”Fundations of quantium computing” str. 97-142 part 1 Archiwum Inf. Teoretycznej i Stosowanej vol 13 (2) 2001, str. 93-106 part 2 Archiwum Inf. Teoretycznej i Stosowanej vol 14 (2) 2002

Abstract

The article presents model using quantum e-voting cards based on protocols of quantum key distribution. The strength of the model is using security based on the laws of physics in a place of computing security. In accordance with the principle of Heisenberg, uncertainty

measurements cannot be made in two databases at the same time, which means that the act of measurement always introduces distortion. In addition, an essential element of the model is the total transparency of dedicated vote (Eve doesn`t know which card has been used so she doesn`t know which of the candidates has been selected). The weakness of the presented model is equipment which is hardly available and very expensive at the moment. However, given the steady progress in the field of mechanics and quantum physics, we can assume that in the near future, this equipment may become available for reasonable money.