ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2014
Seria: ORGANIZACJA I ZARZĄDZANIE z. 74 Nr kol. 1921

Marcin SOBOTA
Wydział Organizacji i Zarządzania
Politechnika Śląska

ANALIZA PORÓWNAWCZA PROTOKOŁÓW BB84 ORAZ SARG

Streszczenie. Artykuł przedstawia analizę porównawczą dwóch kwantowych protokołów uzgadniania klucza szyfrującego: BB84 oraz SARG. Protokół SARG jest rozwinięciem protokołu BB84, usuwa jego brak odporności na niedoskonałość źródła fotonów, które czasem generuje parę identycznych fotonów zamiast pojedynczego fotonu. W pracy opisano budowę obu protokołów.

Słowa kluczowe: analiza porównawcza, protokół kwantowy, protokół BB84, protokół SARG.

COMPARATIVE ANALYSIS OF PROTOCOLS BB84 AND SARG

Summary. Article presents comparative analysis of quantum protocols BB84 and SARG. SARG protocol is an extension of BB84 protocol, removes his lack of resistance to imperfect photon sources, which sometimes generates a pair of identical photons instead of a single photon. This paper describes the construction of these two protocols.

Keywords: Comparative analysis, quantum protocol, BB84 protocol, SARG protocol.

1. Wstęp

Kwantowe protokoły uzgadniania klucza szyfrującego są alternatywą dla algorytmów klucza publicznego. Ponieważ rozwój informatyki kwantowej zagraża metodom klasycznym (budowa komputera kwantowego pozwoliłaby w rozsądnym czasie łamać algorytm RSA), poszukuje się metod, które w razie kompromitacji metod klasycznych przejęłyby funkcje metod pozwalających na bezpieczną komunikację.

W artykule przedstawiono analizę porównawczą dwóch kwantowych protokołów uzgadniania klucza szyfrującego: BB84 oraz SARG. Budowa protokołów jest z jednej strony

bardzo podobna (protokół SARG jest modyfikacją protokołu BB84), z drugiej zaś wprowadzone modyfikacje powodują pojawienie się znaczących różnic. Główną przyczyną konieczności modyfikowania protokołu BB84 był problem z niedoskonałością sprzętu, na którym protokół wykorzystywano. Zgodnie z zasadą nieoznaczoności Heisenberga niemożliwe jest wykonanie pomiarów w dwóch nieortogonalnych bazach jednocześnie. Twierdzenie o nieklonowaniu zabezpiecza przesyłany ciąg fotonów przed wykonaniem kopii nieznanych stanów kwantowych. Natomiast największym problemem jest generowanie przez źródło par identycznych fotonów (fotonów o takiej samej polaryzacji) zamiast pojedynczych fotonów, co oznacza, że strona podsłuchująca ma możliwość wykonania dwóch pomiarów (na każdym z pary identycznych fotonów pomiar jest wykonywany w innej bazie) albo może wykonać pomiar na jednym z nich, przesyłając foton drugi w stanie niezmienionym, a tym samym pozostając niewidoczna.

2. Protokół BB84

Idea wykorzystywana w protokole BB84 [1, 2, 3, 5, 6, 7] została rozwinięta już w latach siedemdziesiątych, ale prace nad nią ukończono w 1984 roku, stąd data w nazwie. Jej twórcami są: Charles Bennett, Gilles Brassard i Artur Ekert. Opiera się ona na zastosowaniu dwóch alfabetów:

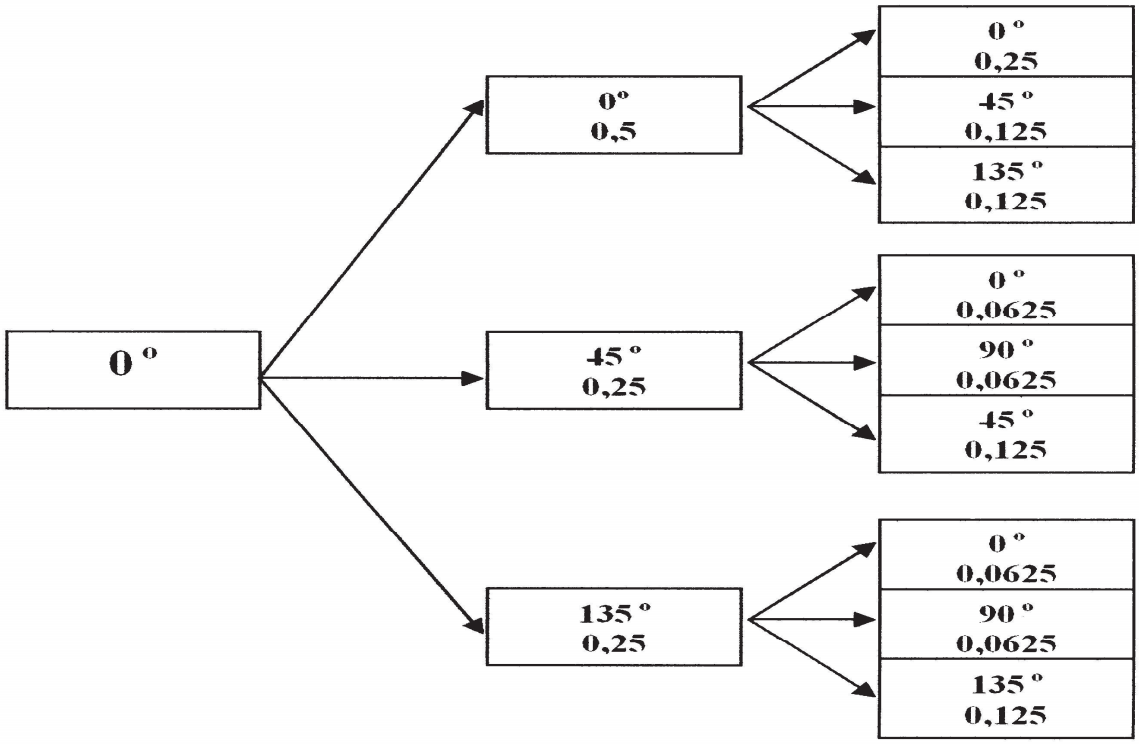
- prostego, zawierającego fotony światła o polaryzacji 0^o i 90^o (odpowiednio binarne 0 i 1),
- ukośnego, zawierającego fotony światła o polaryzacji 45^o i 135^o (odpowiednio binarne 0 i 1).

Konsultacja klucza szyfrującego odbywa się w następujących krokach:

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, Alicja zaś informuje go, czy wybrane losowo typy baz były właściwe, czy nie.
5. 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.

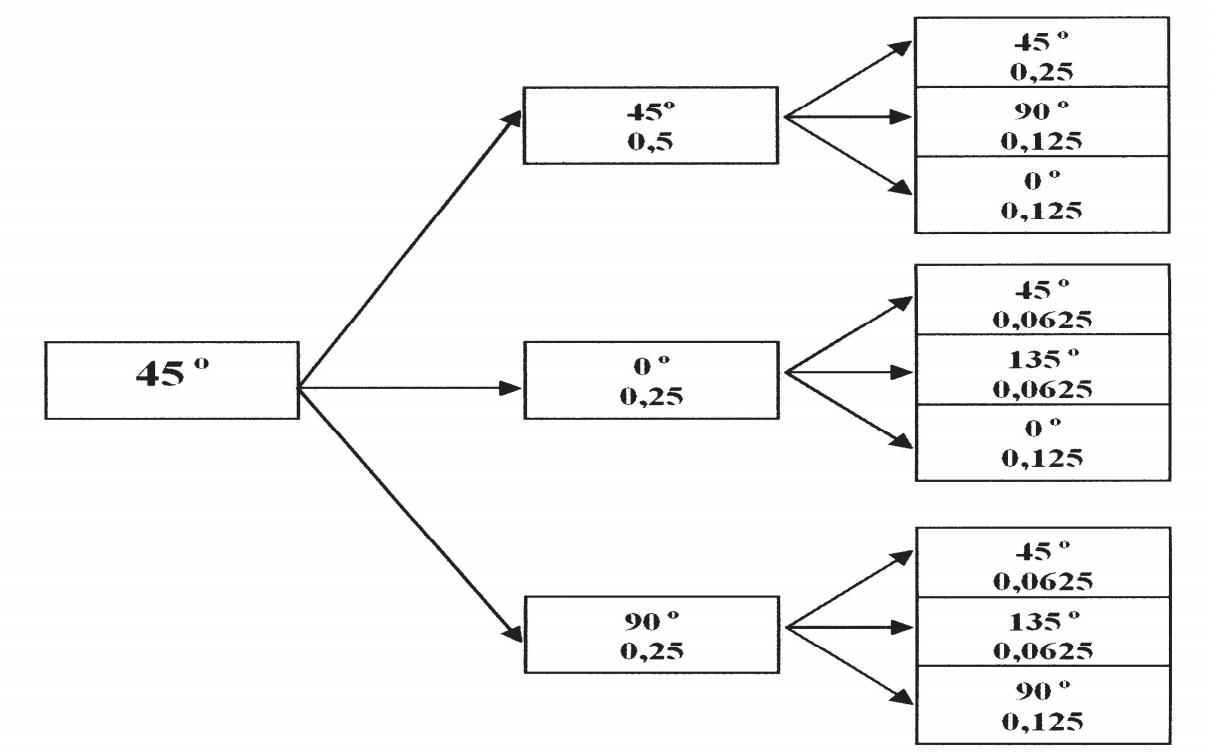
Taki sposób wymiany klucza szyfrującego pozwala na wykrycie podsłuchu na łączu. Wynika to z prawa mechaniki kwantowej, zgodnie z którym nie jest możliwy pasywny

podsłuch. Każdy podsłuch jest aktywny i wprowadza przekłamania w przekazie. Aby wykryć podsłuch, wybiera się pewien ciąg fotonów, na które Bolek i Alicja nałożyli te same bazy, i sprawdza się, czy uzyskano te same wyniki. Jeśli przynajmniej dla jednego fotonu uzyskano różne wyniki mimo nałożenia tych samych baz, to oznacza to, że na łączu wystąpił podsłuch. W takim przypadku konsultację klucza należy rozpocząć od nowa. Jeżeli na łączu występuje podsłuch, to drogę fotonu od wysłania go przez Alicję aż do uzyskania wyniku przez Bolka przedstawiają rysunki 1 i 2. Ścieżkę taką przedstawiono dla fotonu o polaryzacji 0^o i 45^o. Pierwsza kolumna to polaryzacja fotonu wysłanego przez Alicję. Druga kolumna to bazy zastosowane przez Ewę (podsłuchującego) oraz prawdopodobieństwa, z jakimi możliwe są do uzyskania dane wyniki. Trzecia kolumna to bazy zastosowane przez Bolka oraz prawdopodobieństwa, z jakimi uzyskuje on dany wynik po uwzględnieniu występującego podsłuchu. Jeżeli zastosowana baza jest prawidłowa, to polaryzacja uzyskanego fotonu jest taka sama jak fotonu wysłanego. Jeżeli zaś zastosowana baza jest nieprawidłowa, to następuje odwrócenie polaryzacji fotonu, tzn. polaryzacja fotonu z 0^o zostaje zmieniona na 45^o lub 135^o (to samo dotyczy fotonu o polaryzacji 90^o), natomiast polaryzacja fotonu z 45^o zostaje zmieniona na 0^o lub 90^o (analogicznie zmienia się polaryzacja fotonu 135^o).



Rys. 1. Możliwe ścieżki fotonu o polaryzacji prostej od nadawcy do adresata, przy założeniu że występuje podsłuch

Fig. 1. Probably path of photon in linear polarization



Rys. 2. Możliwe ścieżki fotonu o polaryzacji ukośnej od nadawcy do adresata, przy założeniu że występuje podsłuch
Fig. 2. Probably path of photon in diagonal polarization

3. Protokół SARG

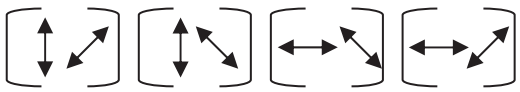
Protokół SARG [4] pod względem struktury jest modyfikacją protokołu BB84. Nieco inaczej kodowane są bity klasyczne oraz przede wszystkim inna jest informacja jawna przesyłana kanałem klasycznym.

Protokół SARG dokładnie tak samo jak protokół BB84 wykorzystuje 4 polaryzacje fotonów (0^o; 45^o; 90^o i 135^o) oraz dwie bazy pomiarowe (prostą i ukośną). Kodowanie jednak wygląda następująco:


klasyczny bit 0


klasyczny bit 1

Ponadto Alicja może ogłosić następujące pary:

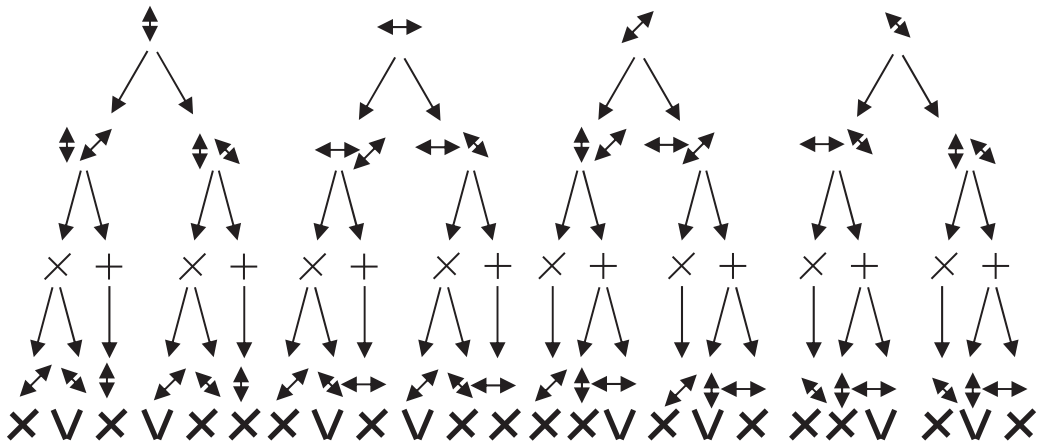


Uzgadnianie klucza odbywa się następująco:

1. Alicja wybiera jedną z czterech możliwych polaryzacji i foton o takiej polaryzacji wysyła do Boba.
2. Alicja ogłasza jednocześnie odpowiednią parę polaryzacji w taki sposób, by zawierała ona polaryzację wybraną przez Alicję oraz dowolną polaryzację z drugiej możliwej bazy. Jeżeli Alicja wybrała np. foton o polaryzacji 90^o, to ogłasza jedną z dwóch możliwych par: $\{90^o; 45^o\}$ lub $\{90^o; 135^o\}$. Dla rozpatrywanego przypadku przyjmijmy, że Alicja wybrała parę $\{90^o; 45^o\}$.
3. Bob nie wie, która z podanych polaryzacji jest prawidłowa, a która została dobrana przez Alicję jako uzupełnienie pary, stąd jego wybór bazy odczytującej jest losowy.
4. Jeżeli Bob zgadł bazę, w jakiej przez Alicję został przesłany foton, to jego odczyt jest deterministyczny, pomiar polaryzacji jest prawidłowy, ale nierozstrzygający. Alicja przesłała foton o polaryzacji 90^o, Bob dokonał odczytu w bazie prostej, co oznacza, że jako wynik otrzymał foton o polaryzacji 90^o. Należy jednak zauważyć, że gdyby w ogłoszonej parze $\{90^o; 45^o\}$, to polaryzacja 45^o była polaryzacja przesłaną przez Alicję, Bob przy wyborze bazy prostej mógłby również uzyskać wynik 90^o. Stąd Bob nadal nie wie, czy jego wybór był prawidłowy.
5. Jeżeli Bob nie zgadł bazy, wybierając bazę nieortogonalną do polaryzacji mierzonego fotonu (w naszym przypadku to wybór bazy ukośnej), może z prawdopodobieństwem ½ uzyskać jeden z dwóch możliwych wyników:
   a) polaryzację 45^o, co również jest wynikiem nierozstrzygającym, ponieważ, podobnie jak w punkcie 4, taki wynik pojawiłby się, gdyby Alicja wysłała foton o polaryzacji 45^o przy wyborze bazy ukośnej przez Boba;
   b) polaryzację 135^o, czyli taką polaryzację, której w ogłoszonej przez Alicję parze nie ma. Ten wynik jest wynikiem rozstrzygającym, oznaczającym jednoznacznie, że Alicja wysłała foton o polaryzacji 45^o.
6. Bob informuje jedynie Alicję, które z uzyskanych przez niego wyników są nierozstrzygające i te bity zostają usunięte z klucza.
7. Ostatnim krokiem jest negacja bitów przez Boba (Alicja zakodowała przez polaryzację 45^o klasyczne 0, natomiast Bob przez pomiar polaryzacji 135^o uzyskał klasyczne 1. Po zanegowaniu bitu Boba wartości po obu stronach komunikacji stają się identyczne.

Wszystkie możliwe do zaistnienia sytuacje przedstawia rys. 3. Przedstawiono na nim kolejno (w poziomie):

- wybór polaryzacji dokonany przez Alicję,
- wybór pary ogłoszonej przez Alicję,
- wybór bazy przez Boba,
- wynik uzyskany przez Boba,
- informacja o tym, czy wynik jest nierozstrzygający (x), czy rozstrzygający (V).



Rys. 3. Możliwe ścieżki fotonów w protokole SARG
Fig. 3. Probably path of photons in SARG protocol

Pozostaje jeszcze kwestia określenia, czy wystąpił podsłuch. Aby to zrobić, Alicja i Bob muszą sprawdzić polaryzacje fotonów, dla których Bob użył baz prawidłowych (czyli np. dla polaryzacji 0^o lub 90^o bazy prostej). Jeżeli uzyskane wyniki zgadzają się z polaryzacjami wysłanymi przez Alicję, to znaczy, że kanał dystrybucji nie był podsłuchiwany. W przypadku stwierdzenia podsłuchu komunikację należy rozpocząć od nowa.

4. Podsumowanie

Protokół BB84 efektywniej[1] wykorzystuje generowane bity, ok. 50% może zostać wykorzystanych w kluczu, podczas gdy w protokole SARG jedynie 25% początkowo generowanych fotonów może zostać prawidłowo odczytanych i wykorzystanych. Jak wspomniano na wstępie, protokół SARG jest oparty na protokole BB84 i różni się od niego jedynie sposobem kodowania oraz rodzajem danych przesyłanych kanałem otwartym. Ta różnica powoduje jednak, że protokół SARG staje się bardziej odporny na atak typu PNS. O ile w przypadku protokołu BB84 generowanie podwójnych fotonów stanowi duże zagrożenie dla bezpieczeństwa komunikacji, o tyle w przypadku protokołu SARG zagrożenie to pojawi się dopiero w momencie generowania trójek identycznych fotonów, a ta sytuacja zdarza się dużo rzadziej. Zważywszy na fakt, iż protokoły kwantowe wykorzystuje się wszędzie tam, gdzie poziom bezpieczeństwa musi być bardzo wysoki, oraz pamiętając o tym, że protokoły te służą jedynie do uzgodnienia kluczy szyfrujących dla klasycznych algorytmów kryptograficznych, można uznać, że zdecydowanie bardziej uzasadnione jest

[1] Efektywność jest rozumiana jako stosunek liczby wygenerowanych bitów do liczby bitów, które mogą zostać wykorzystane w kluczu szyfrującym.

wykorzystywanie protokołu SARG – zapewnia wyższy poziom bezpieczeństwa przy, co prawda, niższej efektywności, lecz jak wspomniano, efektywność nie jest dla tych protokołów cechą najważniejszą.

Bibliografia

1. Bennett C.H., Brassard G., 1984: Quantum Cryptography: Public Key Distribution and Coin Tossing. Proceedings of IEEE International Conference on Computers Systems and Signal Processing. Bangalore India.
2. Tamaki K., Lutkenhaus N., 2004: Unconditional Security of the Bennett 1992 quantum key-distribution protocol over a lossy and noisy chanel. Phys. Rev. A, no. 69, 032316.
3. Tamaki K., Koashi M., Imoto N., 2003: Unconditional Security of the Bennett 1992 quantum key-distribution protocol over a lossy and noisy chanel. Phys. Rev. Lett., no. 90, 167904.
4. Scarani V. et al., 2004: Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations. Phys. Rev. Lett. 92.
5. Białas A. i inni, 2010: Klasyczne i kwantowe metody podniesienia bezpieczeństwa informacji w systemach komputerowych. WSB w Dąbrowie Górniczej.
6. Kapczyński A., Sobota M., 2008: Kryptografia kwantowa i biometria jako rozwinięcie klasycznych metod ochrony informacji. Gliwice, Politechnika Śląska.
7. Klamka J., Węgrzyn S.: Kwantowe systemy informatyki, Studia Informatica, vol. 21, no. 1, (39), 2000, p. 15-45.

Abstract

This article presents a comparative analysis of protocols BB84 and B92. SARG protocol is a modification of the BB84 protocol. The differences between construction of these protocols makes the SARG protocol more resistant to PNS attack and thus SARG provides a higher level of security. Although the effectiveness of the SARG protocol is lower than effectiveness of BB84 protocol, but in QKD protocols most important is level of security.