ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2011
Seria: ORGANIZACJA I ZARZĄDZANIE z. 57 Nr kol. 1847

Marcin SOBOTA
Politechnika Śląska
Wydział Organizacji i Zarządzania
Instytut Ekonomii i Informatyki

MODEL UZGADNIANIA KLUCZA SZYFRUJĄCEGO METODAMI KWANTOWYMI DLA DOWOLNYCH ODLEGŁOŚCI

Streszczenie. Artykuł dotyczy istotnego problemu, związanego z ograniczeniem odległości, na jaką może zostać przesłany klucz kryptograficzny, przy zastosowaniu do tego celu kwantowych metod uzgadniania klucza szyfrującego. Przedstawiono w nim model uzgadniania klucza pozwalający przekroczyć granicę wyznaczoną przez dwa komunikujące się urządzenia kwantowe.

MODEL KEY AGREEMENT CRYPTOGRAPHIC METHOD FOR ANY DISTANCE QUANTUM

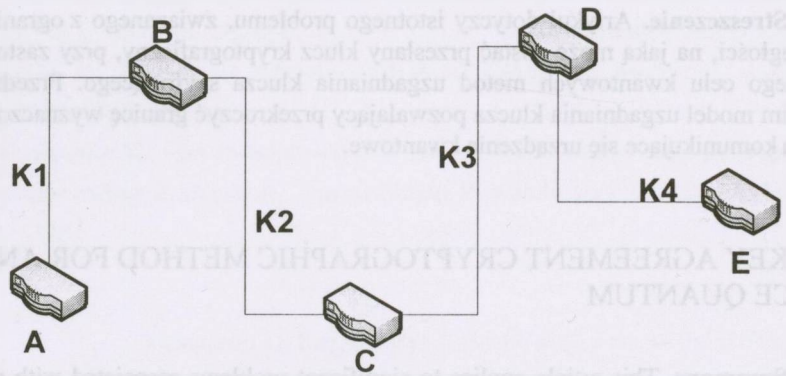
Summary. This article applies to significant problems associated with restricted range, on which a cryptographic key can be send to, using for this purpose, the methods of quantum encryption key agreement. It presents a model of key agreement to exceed the limit fixed by the two communicating devices quantum

1. Wstęp

Kwantowe metody uzgadniania klucza szyfrującego są najnowszymi i najbezpieczniejszymi sposobami na przesłanie klucza symetrycznego, który ma posłużyć do szyfrowania wiadomości [1, 2, 3, 4, 5, 6, 9, 10]. Dzięki temu, że bezpieczeństwo zapewnia fizyka kwantowa (na poziomie kwantowym nie można wykonać pasywnego podsłuchu) metody te gwarantują wyższy poziom bezpieczeństwa niż klasyczne algorytmy asymetryczne, zapewniające bezpieczeństwo obliczeniowe. Problemem jest jednak ograniczenie odległości, na jaką może zostać wysłany klucz.

2. Stan aktualny

Komercyjne rozwiązania, pozwalające wykorzystać fizykę kwantową do zapewniania bezpiecznego uzgadniania klucza szyfrującego, wymagają zastosowania tzw. ciemnych światłowodów. Pojęcie to oznacza, że na drodze między nadajnikiem a odbiornikiem nie może pojawić się żadne urządzenie aktywne, które pozwoliłoby wzmocnić sygnał. Determinującymi czynnikami, określającymi maksymalne odległości dla tego rodzaju komunikacji, są więc moc nadajnika oraz tłumienność łącza. W praktyce oznacza to, że maksymalna odległość, na jakiej może odbywać się uzgadnianie klucza, wynosi ok. 100 km [7, 8, 11]. W czasach dzisiejszej globalizacji jest to wynik wysoce niezadowalający. Podejmuje się więc próby zwiększenia tej odległości. Realizowane rozwiązanie polega na ustawianiu wielu stacji pośrednich, które uzgadniają między sobą klucz metodami kwantowymi. Model takiego uzgadniania przedstawia rys 1.



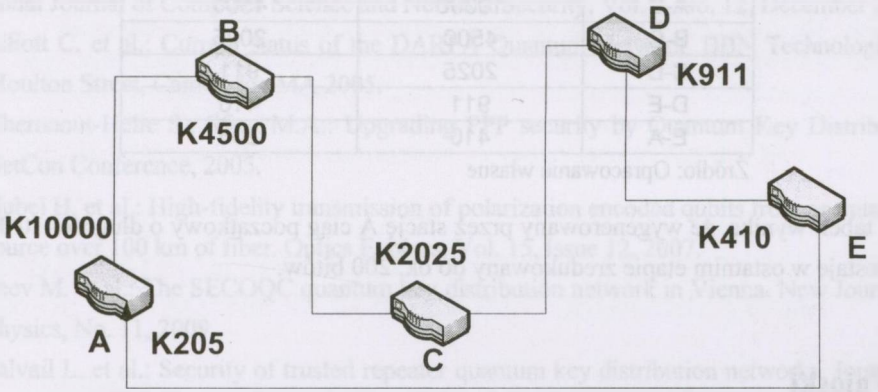
Rys. 1. Schemat uzgadniania klucza szyfrującego metodami kwantowymi
Fig. 1. Scheme of quantum key agreement
Źródło: Opracowanie własne

Jeśli stacja A chce przesłać do stacji E, oddalonej o ok. 400 km, zaszyfrowaną wiadomość wykorzystującą klucz symetryczny uzgodniony metodami kwantowymi, musi to zrobić poprzez stacje pośrednie. Nawiązuje łączność ze stacją B, oddaloną do 100 km, i uzgadnia z nią klucz K1. Stacja B nawiązuje łączność ze stacją C, oddaloną do 100 km od stacji B, i uzgadnia z nią klucz K2. Takim samym sposobem i dla takich samych warunków uzgadniają klucze stacje C z D oraz D z E. Jeśli na całej trasie klucze są uzgodnione, można przejść do przesłania wiadomości szyfrowanej uzgodnionymi kluczami. Podstawowym problemem tego sposobu komunikacji jest to, że każda ze stacji pośrednich bierze udział nie tylko w uzgadnianiu klucza, ale również w przesyłaniu tajnej wiadomości. Każda stacja pośrednia musi tajną wiadomość deszyfrować, by następnie zaszyfrować ją kluczem uzgodnionym ze stacją kolejną. Oznacza to, że każda stacja pośrednia wie, jaka wiadomość jest przesyłana,

mimo że nie jest jej bezpośrednim adresatem. Poddaje to w wątpliwość bezpieczeństwo wiadomości w całym procesie komunikacji.

3. Proponowane zmiany

Istotnym elementem poprawiającym bezpieczeństwo przesyłanych informacji jest zapewnienie bezpośredniej komunikacji między stacjami końcowymi. W chwili obecnej nie ma możliwości zwiększenia odległości, na jakiej odbywa się komunikacja, bez wykorzystania stacji pośrednich. Dokonując jednak pewnej modyfikacji modelu, można spowodować, że po uzgodnieniu klucza komunikować będą się już jedynie stacje końcowe, z pominięciem stacji pośrednich. Nowy model uzgadniania klucza szyfrującego przedstawiono na rys. 2. Liczby oznaczają długości ciągów bitów po wykonaniu procedury uzgadniania.



Rys. 2. Poprawiony model uzgadniania klucza szyfrującego metodami kwantowymi
Fig. 2. Improved model of quantum key agreement
Źródło: Opracowanie własne

W zmienionym modelu uzgadniania klucza szyfrującego zastosowano ciąg nadmiarowy. Stacja A musi przewidzieć, jaka będzie wymagana długości klucza szyfrującego pozwalającego na zaszyfrowanie wiadomości dla stacji E. Biorąc pod uwagę „straty" wynikające z budowy protokołu kwantowego, stacja A generuje ciąg odpowiedniej długości. Dodatkowo, każdy z wysłanych fotonów otrzymuje identyfikujący go indeks, tak by po ostatniej sesji (stacji D ze stacją E) wiadomo było, które z początkowych fotonów (wysłanych przez stację A) posłużyły do utworzenia klucza szyfrującego. Oczywiście nie zostaną wykorzystane te same fotony, a jedynie odpowiednie polaryzacje.

Pierwsze uzgodnienie realizują stacje A i B. Uzgodniony klucz będzie miał długość stanowiącą ok. 45% liczby fotonów wysłanych przez stację A. Te 45% prawidłowych i uzgodnionych polaryzacji zostanie wykorzystanych przez stację B do uzgadniania klucza ze stacją

C. Tutaj również nastąpi redukcja liczby fotonów, które zostaną wykorzystane do utworzenia klucza. Proces ten powtarza się aż do uzgodnienia klucza między stacjami D i E. Następnie, stacja E kontaktuje się ze stacją A, informując ją, które z początkowych fotonów posłużyły do uzgodnienia klucza między stacjami D i E. Wykorzystuje do tego indeksy fotonów. Dodatkowo, stacje E i A mogą postanowić, że wykorzystywany przez nie klucz będzie podzbiorem klucza uzgodnionego między stacjami D i E, tak aby stacja D również nie wiedziała, jaki klucz zostanie wykorzystany do zaszyfrowania wiadomości przesyłanej między stacjami E i A. Redukcja ciągów fotonów pokazana jest w tab. 1.

Tabela 1

Redukcja ciągów fotonów na poszczególnych etapach

Uzgodnienie (stacje)	Długość generowanego ciągu (liczba fotonów)	Długość uzgodnionego klucza (bity)
A-B	10000	4500
B-C	4500	2025
C-D	2025	911
D-E	911	410
E-A	410	205

Źródło: Opracowanie własne

Z tabeli wynika, że wygenerowany przez stację A ciąg początkowy o długości 10 000 bitów zostaje w ostatnim etapie zredukowany do ok. 200 bitów.

4. Wnioski

Aktualnie wykorzystywany model uzgadniania klucza szyfrującego metodami kwantowymi dla odległości przekraczającej 100 km zakłada, że należy utworzyć odpowiednią liczbę stacji pośrednich oddalonych od siebie o maksymalnie 100 km. Stacje uzgadniają miedzy sobą klucze, które następnie wykorzystują do szyfrowania wiadomości. Przy takim podejściu pojawiają się dwa zasadnicze problemy: w samym procesie szyfrowania uczestniczą wszystkie stacje pośrednie oraz każda ze stacji pośrednich zna treść przesyłanej wiadomości (każda stacja musi wiadomość deszyfrować kluczem uzgodnionym ze stacją poprzedzającą, by następnie zaszyfrować ją kluczem uzgodnionym ze stacją następną).

Zaproponowany przez autora model rozwiązuje te problemy. Wykorzystanie ciągu nadmiarowego powoduje w ostatniej fazie możliwość uzgodnienia klucza znanego jedynie stacjom końcowej i początkowej, co z kolei powoduje, że możliwe jest ominięcie stacji pośred-

nich w procesie szyfrowania (co znacznie przyspiesza cały proces) oraz treść wiadomości znana jest jedynie stacjom do tego uprawnionym.

BIBLIOGRAFIA

1. Dianati M., Alléaume R.: Architecture of the secoqc Quantum Key Distribution Network. ICQNM, IEEE Computer Society Press, 2007.
2. Dixon A.R. et al.: Continuous operation of high bit rate quantum key distribution. Applied Physics Letters American Institute of Physics, 2010.
3. Duan L.-M. et al.: Long-distance quantum communication with atomic ensembles and linear optics. Nature, No. 414, 2001.
4. Elboukhari M. et al.: Integration of quantum key distribution in the TLS protocol. International Journal of Computer Science and Network Security, Vol. 9, No. 12, December 2009.
5. Elliott C. et al.: Current status of the DARPA Quantum Network. BBN Technologies 10 Moulton Street, Cambridge MA 2005.
6. Ghernaout-Helie S., Sfaxi M.A.: Upgrading PPP security by Quantum Key Distribution. NetCon Conference, 2005.
7. Hubel H. et al.: High-fidelity transmission of polarization encoded qubits from an entangled source over 100 km of fiber. Optics Express, Vol. 15, Issue 12, 2007.
8. Peev M. et al.: The SECOQC quantum key distribution network in Vienna. New Journal of Physics, No. 11, 2009.
9. Salvail L. et al.: Security of trusted repeater quantum key distribution networks. Journal of Computer Security, No. 18(1), 2010.
10. Salvail L. et al.: Security of Trusted Repeater Quantum Key Distribution Networks. Journal of Computer Science, Special Issue on the European ICT Security Projects of the FP6, 2009.
11. Stucki D., Gisin N., Guinnard O., Ribordy G., Zbinden H.: Quantum key distribution over 67 km with a plug & play system. New Journal of Physics, No. 4, 41, 2002.

Recenzent: Dr hab. inż. Ireneusz J. Jóźwiak

Abstract

Model currently used for key agreement methods of quantum encryption, for a distance exceeding 100 km implies that you must create a sufficient number of intermediate stations placed by a maximum of 100 km from each other. Stations agree between themselves the keys, who then use to encrypt messages. With this approach there are two main problems: in the encryption process there are all intermediate stations involved and they all are familiar with the content of the message (each station must decrypt the message by using a key agreed with the previous station and then encrypt it with a key agreed with the next station.)

Model suggested by the author solves these problems. Use of the redundancy makes it possible to agree, in the last phase, the key known only to the stations: the final and initial which makes it possible to bypass intermediate stations in the encryption process (which speeds up the process) and the message is known only to stations authorized to do so.