Piotr BILSKI, Wiesław WINIECKI
POLITECHNIKA WARSZAWSKA,
ul. Nowowiejska 15/19, 00-665 Warszawa

Analiza możliwości wykorzystania obliczeń kwantowych do realizacji bezpiecznego systemu pomiarowego

Dr inż. Piotr BILSKI

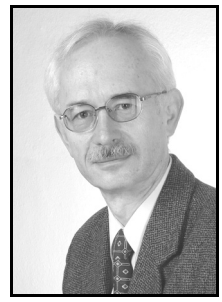
Piotr Bilski (ur. 1977 w Olsztynie) uzyskał w 2000 r. tytuł inżyniera, w 2001 r. magistra, a w 2006 r. doktora (dwa ostatnie z wyróżnieniem) na Wydziale Elektroniki i technik Informacyjnych Politechniki Warszawskiej. Obecnie jest adiunktem w Instytucie Radioelektroniki oraz na Wydziale Zastosowań Informatyki i Matematyki SGGW. Jego zainteresowania naukowe obejmują diagnostykę systemów analogowych, analizę i projektowanie komputerowych systemów pomiarowych oraz zastosowania sztucznej inteligencji w naukach przyrodniczych.

e-mail: pbilski@elka.pw.edu.pl, piotr_bilski@sggw.pl

Prof. nzw. dr hab. inż. Wiesław WINIECKI

Prof. nzw. na Wydziale Elektroniki i Technik Informacyjnych PW. Kierownik zespołu Komputerowej Techniki Pomiarowej. Autor lub współautor 4 książek i ponad 150 publikacji naukowych. Obszary zainteresowań: systemy pomiarowe, przyrządy wirtualne, nowoczesne technologie komunikacyjne i programowe w skupionych i rozproszonych systemach pomiarowo-kontrolnych. Prezes POLSPAR, członek Komitetu Metrologii PAN, członek IEEE.

e-mail: W.Winiecki@ire.pw.edu.pl



Streszczenie

W artykule przedstawiono analizę możliwości wykorzystania obliczeń kwantowych do zapewnienia bezpieczeństwa transmisji i przetwarzania danych w rozproszonym systemie pomiarowym. Omówiono zagrożenia dla poufności danych w takim systemie oraz ich źródła. Przedstawiono ideę komputera kwantowego i kwantowego kanału transmisyjnego oraz potencjalne sposoby wykorzystania ich w celu zapewnienia bezpieczeństwa danych pomiarowych i sterujących.

Słowa kluczowe: systemy pomiarowe, algorytmy kwantowe, kryptografia kwantowa.

Analysis of designing the quantum computing-based secure measurement system

Abstract

The paper deals with the analysis of possible implementation of the quantum computations to ensure security of data transmission and processing in the distributed measurement system. Firstly, sources of security threats (mainly the transmission media) in the typical system are presented. Then, two applications of quantum computing are presented to defend the system against the intruders. The first one, the quantum transmission channel, is reliable, safe and can be implemented using today technology. The paper describes the BB84 algorithm that ensures the safe data transfer. Another one, the quantum computer, is a device of novel computational capabilities, which can be used to break contemporary cryptographic systems (such as RSA). The paper considers possible cryptographic algorithms that could be resilient to the attack using such device. All methods are discussed from the measuring systems point of view and refer to their specific characteristics. Finally, conclusions and future prospects are presented.

Keywords: measurement system, quantum algorithms, quantum cryptography.

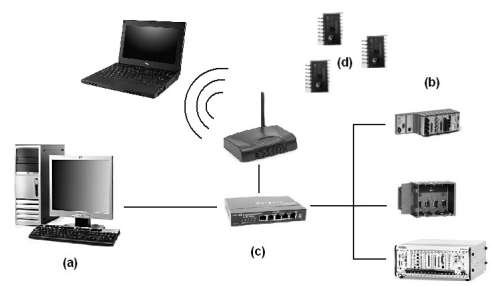
1. Wstęp

Współczesne rozproszone systemy pomiarowo-kontrolne (RSPK) w znaczącym stopniu oparte są na komputerowych technikach obliczeniowych. Pozyskiwanie danych pomiarowych oraz ich przetwarzanie wykorzystuje zarówno komputery ogólnego przeznaczenia, jak i specjalizowane systemy wbudowane i mikrokontrolery. W kanale transmisyjnym może dojść do przechwycenia lub nieautoryzowanej modyfikacji danych. Ze względu na upowszechnienie się systemów pomiarowo-kontrolnych w dziedzinach życia istotnych dla ludności (elektrownie, zarządzanie ruchem miejskim, stacje dystrybucji wody) istotnym problemem staje się zapewnienie bezpiecznej pracy takiego systemu. Wymienione obiekty mogą stać się np. celem ataku terrorystów, więc ich zabezpieczenie przed niepowołanym dostępem staje się ważnym zadaniem, któremu należy poświęcić więcej uwagi. Pojawienie się nowych architektur komputerowych może sprawić, że klasyczne metody zabezpieczania danych oraz ich transmisji (oparte na technikach kryptograficznych) staną się nieskuteczne.

Obecnie uważa się, że największym problemem będzie wprowadzenie do użytku komputerów kwantowych. Prezentują one właściwości naruszające bezpieczeństwo wielu stosowanych obecnie algorytmów. Należy dokonać analizy bezpieczeństwa współczesnych RSPK i rozważyć modyfikacje zapewniające poufność informacji, pomimo wykorzystania takiego urządzenia do ataku. W artykule przedstawiono możliwości zapewnienia bezpieczeństwa w RSPK z uwzględnieniem obliczeń kwantowych, zarówno po stronie zarządcy systemu, jak i intruza. W punkcie 2 przedstawiono architekturę współczesnego RSPK i wskazano jego słabe punkty pod względem bezpieczeństwa. W punkcie 3 zawarto wprowadzenie do obliczeń kwantowych. Punkt 4 zawiera propozycję realizacji bezpiecznego kanału transmisyjnego z użyciem obliczeń kwantowych. Z kolei opis możliwości obrony systemu przed atakiem kryptoanalitycznym z użyciem komputera kwantowego, który jest jeszcze na etapie rozważań teoretycznych, znajduje się w punkcie 5. Punkt 6 zawiera podsumowanie i wnioski.

2. Bezpieczeństwo w RSPK

Typowa architektura RSPK (rys. 1) składa się z elementów sterujących (a) wykonawczych (b) oraz infrastruktury komunikacyjnej (c) [1]. Wymaga ona zabezpieczenia z dwóch względów.



Rys. 1. Architektura RSPK: moduł sterujący (a), moduły wykonawcze (b), infrastruktura komunikacyjna (c), sieci czujnikowe (d)
Fig. 1. Distributed measurement system architecture: control module (a), measurement module (b), communication infrastructure (c), sensory networks (d)

Pierwszy to uniemożliwienie dostępu do kanału transmisji danych. W przypadku zastosowania technik przewodowych (np. sieć komputerowa standardu IEEE 802.3), przechwycenie danych możliwe jest po fizycznym podłączeniu się do systemu, co jest trudne w realizacji. Popularność zyskuje transmisja bezprzewodowa (standard IEEE 802.11 lub ZigBee), której wykorzystanie ułatwia nieautoryzowane podłączenie do systemu. Drugi aspekt wymaga uniemożliwienia odczytania danych w przypadku ich przechwycenia. Jest to typowy problem kryptologiczny, wymagający zastosowania algorytmów szyfrujących i deszyfrujących do

danych pomiarowych przesyłanych z węzłów wykonawczych oraz informacji sterującej przesyłanych do nich z węzła sterującego. Do wykonywania operacji szyfrowania potrzebna jest moc obliczeniowa, rozłożona w RSPK niesymetrycznie. Moduły sterujące dysponują szybszymi procesorami, niż jednostki wykonawcze.

Algorytmy kryptograficzne należą do jednej z dwóch grup metod. Metody symetryczne wykorzystują ten sam klucz do zamiany jawnej informacji (tutaj danych pomiarowych lub sterujących) na szyfr, i operacji odwrotnej. Z tego względu istotne jest utrzymywanie go w tajemnicy. Najpopularniejsze algorytmy symetryczne (do wykorzystania w RSPK) to DES, AES i IDEA. Metody asymetryczne wykorzystują dwa klucze: jeden służy do szyfrowania, drugi do deszyfrowania. W zależności od zastosowania jeden z nich jest jawny, drugi musi być utrzymywany w tajemnicy. Najpopularniejsze algorytmy asymetryczne to RSA, czy ElGamal.

3. Obliczenia kwantowe

Rozwój nauk fizycznych w ciągu ostatnich lat umożliwił zaproponowanie nowego rodzaju obliczeń z wykorzystaniem mechaniki kwantowej. Urządzeniem, które wykorzystuje to zjawisko, jest komputer kwantowy. Istotą obliczeń jest stan kwantowy, reprezentowany przez podstawową jednostkę informacji – bit kwantowy (kubit), reprezentowany przez superpozycję dwóch stanów [2]:

$$|\Psi\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle, \tag{1}$$

gdzie obydwa stany $|0\rangle$ i $|1\rangle$ są wektorami:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{2}$$

i występują jednocześnie, zaś α i β to liczby zespolone takie, że:

$$|\alpha|^2 + |\beta|^2 = 1. \tag{3}$$

Wyznaczają one amplitudy prawdopodobieństw (wartości funkcji falowej opisującej każdy układ kwantowy) znalezienia się systemu w stanie, odpowiednio, $|0\rangle$ lub $|1\rangle$. Ponieważ amplitudy w przeciwieństwie do prawdopodobieństw mogą być liczbami ujemnymi (przy spełnieniu warunku (3)), układy kwantowe zachowują się inaczej, niż ich klasyczne odpowiedniki. Eksperymentalnym przykładem jest interferometr Macha-Zhandera [5], w którym przejście fotonu przez jedną z czterech możliwych dróg nie jest tak samo prawdopodobne, ponieważ w dwóch przypadkach amplitudy się znoszą (tzw. interferencja kwantowa).

Ważną cechą obliczeniową jest paralelizm kwantowy, czyli możliwość przetwarzania wszystkich stanów jednocześnie. O ile pojedynczy kubit to dwa stany, dwa kubity opisują cztery stany, trzy kubity – osiem itd. Dzięki temu komputer kwantowy jest w stanie przetwarzać znacznie więcej informacji jednocześnie, niż komputer klasyczny. Wykazano, że algorytmy kwantowe rozwiązują pewne problemy (np. przeszukiwanie drzew, sortowanie [6] lub znajdowanie ukrytych symetrii [7]) znacząco szybciej, niż ich klasyczne odpowiedniki. Pomimo iż uważa się, że komputery kwantowe nie będą w stanie rozwiązywać problemów NP-zupełnych, mogą one znacząco wpłynąć na wymagania wobec systemów kryptograficznych w przyszłości (patrz punkt 4).

Z punktu widzenia bezpieczeństwa RSPK komputer kwantowy może zostać wykorzystany do złamania systemów kryptograficznych chroniących dane przesyłane pomiędzy węzłami systemu pomiarowego. Bez względu na medium transmisji danych, przechwycenie zaszyfrowanych informacji jest możliwe obecnie przy użyciu standardowych urządzeń i technik. Uzyskanie na tej podstawie danych w postaci jawnej okazuje się jednak niemożliwe ze względu na ogromną ilość obliczeń potrzebną do tego celu. Wprowadzenie komputera kwantowego może spowodować, że część stosowanych systemów kryptograficznych przestanie być bezpieczna, jak to opisano w punkcie 5.

4. Kryptografia kwantowa

Zapewnienie bezpieczeństwa transmisji w RSPK może zostać zrealizowane przy użyciu narzędzi kryptografii kwantowej do zbudowania bezpiecznego kanału komunikacyjnego. Podstawą do tego jest właściwość stanu kwantowego, według której pojedynczy kubit pozostaje w nieznanym stanie (tzn. nie są znane amplitudy prawdopodobieństw α i β) do momentu dokonania jego pomiaru. Wówczas ulega on nieodwracalnej zmianie. Nie jest możliwe kopiowanie kubitu, który znajduje się w nieznanym stanie. Z tego powodu przesyłanie kubitów może być przeprowadzone bez obawy, że intruz je zmodyfikuje. Zastosowanie kwantowego protokołu kryptograficznego (najpopularniejszym jest obecnie BB84, choć zaproponowano inne podejścia, np. protokół 6-stanowy i EPR [4]) utrudnia skuteczne odczytanie zawartości przesyłanych kubitów. Zakłada się, że zarówno instrukcje sterujące (polecenia dla urządzeń), jak i dane pomiarowe (zmierzone wielkości), reprezentowane są jako liczby w formacie binarnym.

Protokół BB84 wymaga przesyłania klasycznych zer i jedynek poprzez stany kwantowe, związane z polaryzacją (spinami) pojedynczych fotonów o ustalone z góry wartości (gdzie jeden foton przenosi informację o wartości pojedynczego bitu). W wyniku tego otrzymanie przez odbiorcę zera lub jedynki zależą od polaryzacji, których użyły obie strony komunikacji. Wykorzystywane stany kwantowe to: $|\nearrow\rangle$, $|\searrow\rangle$, $|\uparrow\rangle$, $|\rightarrow\rangle$, które oznaczają wartości polaryzacji, wynoszące 45 stopni, 135 stopni, 0 stopni oraz 90 stopni. Nadawca wykorzystuje wszystkie cztery, odbiorca zaś wykonuje obrót tylko o 0 lub 45 stopni. Wybór polaryzacji przy wysyłaniu poszczególnych bitów odbywa się losowo. Możliwe jest osiem kombinacji, przedstawionych na rys. 2, gdzie „*Nad*" oznacza Nadawcę, „*Odb*" – Odbiorcę, a„–" jest wartością nieokreśloną (0 i 1 są równie prawdopodobne). Zawsze po odebraniu bitu można określić, czy jego wartość była wymuszona przez konfigurację polaryzacji, czy też została ustalona przypadkowo.

Protokół zakłada, że odbiorca przed odebraniem bitu zapisuje polaryzację, jakiej użył i informuje publicznie o tym nadawcę. Wówczas nadawca informuje odbiorcę, które bity z odebranych przez niego miały wartości ustalone zgodnie z rys. 2 (wartości pozostałych są przypadkowe). Obie strony uzyskują przypadkowy ciąg bitów, będący kluczem. Jego przekazanie pomiędzy stronami komunikacji jest realizowalne pod warunkiem odseparowania kanału komunikacyjnego od świata zewnętrznego (w celu uniknięcia przypadkowych zmian wartości kubitów). Ze względu na komplementarność polaryzacji 0 i 90 stopni oraz 45 i 135 stopni, nie jest możliwe przechwycenie danych w RSPK przez intruza bez ujawniania swojej obecności [5]. Nie wie on, które bity są istotne (tzn. ich wartości wynikają z rys. 2). W przypadku pojedynczego bitu intruz ma 50% szans na odgadnięcie prawidłowej polaryzacji. W przypadku dwóch bitów prawdopodobieństwo maleje do 25% itd. Protokół BB84 ma charakter probabilistyczny - w przypadku długich ciągów bitów prawdopodobieństwo poznania informacji maleje do zera. Aby upewnić się, że intruz nie przechwycił danych, nadawca i odbiorca poświęcają część bitów klucza, wymieniając ich wartości. Za cenę uzyskania krótszego (tzw. przesianego [8]) klucza uzyskuje się pewność, że jest on bezpieczny.

Nad. \ Odb.	0	45
0	1	–
45	–	0
90	1	–
135	–	0

Rys. 2. Zasada przypisania bitów zastosowanym obrotom w protokole kwantowym
Fig. 2. Method of the bit assignment to the applied spins in the quantum protocol

Realizacja praktyczna kryptograficznego kanału komunikacyjnego możliwa jest z wykorzystaniem układów optycznych. Istnieją obecnie rozwiązania komercyjne, w których jako źródła fotonów wykorzystywane są lasery, np. słabe impulsy świetlne lub działa fotonowe. Ponieważ protokół kwantowy działa na pojedynczych fotonach, problemem jest maksymalizacja wykorzystania

liczby generowanych cząstek do transmisji z uwzględnieniem możliwości ich rejestracji przez detektory.

Drugim problemem z punktu widzenia RSPK jest korekcja błędów, która jest konieczna ze względu na niedoskonałości medium transmisyjnego. W optycznych kanałach komunikacyjnych stopa błędu (Bit Error Rate - BER) wynosi 10e-9 [8]. Obecne technologie kryptografii kwantowej zapewniają stopę błędu rzędu 2-3 procent, zatem w celu podniesienia jej do akceptowalnego poziomu stosowane jest wzmocnienie prywatności (ang. privacy amplification), prowadzące do kwantowego protokołu korekcji QBER.

Współczesne RSPK mogą mieć różny zasięg, od pojedynczej sieci lokalnej, po system globalny, z komunikacją przez intersieć. Zasięg kwantowego kanału kryptograficznego ma więc istotne znaczenie praktyczne. Obecnie możliwe jest przesyłanie danych tą metodą na odległości setek kilometrów, co jest zbyt kosztowne do zastosowań na dużą skalę. Kryptografia kwantowa znalazła zastosowanie w bankowości [9]. Jako medium transmisyjne można wykorzystać w niej światłowody (co ma wpływ na wybór długości fali świetlnej – 800, 1300 lub 1550 nm), lub powietrze. W celu minimalizacji kosztów RSPK wybór długości fali powinien być podyktowany istnieniem odpowiednich detektorów fotonów (aktualnie najlepsze urządzenia działają dla światła o długości 800 nm) [8]. Tworzenie RSPK o zasięgu globalnym wymaga zapobiegania tłumieniu fali świetlnej, które spowodowane jest ograniczeniami światłowodu (zmniejszenie amplitudy o połowę po 15 km dla przewodu 1550 nm) lub warunkami atmosferycznymi i przeszkodami terenowymi w przypadku powietrza [10].

Dodatkowym aspektem utrudniającym projektowanie RSPK z użyciem kryptografii kwantowej jest często konieczność zapewnienia niewielkich rozmiarów oraz ograniczonego poboru mocy niektórych elementów, co w szczególności dotyczy sieci czujnikowych oraz elementów wykonawczych i pomiarowych umieszczanych w miejscach trudno dostępnych dla człowieka. Obecnie rozwiązania sprzętowe nie spełniają tych wymagań, jednak w przyszłości należy się spodziewać miniaturyzacji i zmniejszenia mocy wymaganej do działania źródeł i detektorów fotonów.

5. Obrona przed algorytmami kwantowymi

Drugim aspektem zapewnienia bezpieczeństwa w RSPK jest zabezpieczenie się przed atakiem przy użyciu komputera kwantowego. Pomimo iż nie udało się dotychczas zbudować urządzenia, które miałoby istotną praktyczną przydatność (istnieją komputery o mocy obliczeniowej do 10 kubitów), odkrycia teoretyczne algorytmów kwantowych (oraz ich weryfikacja na symulatorach [6]) zmuszają do rewizji aktualnie wykorzystywanych systemów kryptograficznych. Ze względów praktycznych w RSPK powinny być rozważane systemy symetryczne, które uważa się za odporne na atak przy użyciu komputera kwantowego. Głównym problemem jest tu dystrybucja klucza, który musi zostać w zaufany sposób dostarczony do wszystkich stron transmisji. Do tego celu wykorzystuje się system asymetryczny, taki jak RSA. Bezpieczeństwo tego systemu oparte jest na założeniu, że niemożliwa jest łatwa faktoryzacja (rozłożenie na czynniki pierwsze) liczby, na której opiera się klucz. Bezpieczeństwo RSA opiera się na długości klucza. W wyniku ciągłego rozwoju technologii komputerowych łamane są coraz dłuższe klucze (ostatnią skuteczną próbą był atak na system z kluczem 768-bitowym [11]). Do 2014 roku planuje się wycofać z użytku RSA z kluczem 1024-bitowym.

Wprowadzenie do użytku komputera kwantowego może uczynić RSA bezużytecznym bez względu na długość klucza, za sprawą algorytmu Shora [3]. Pozwala on na faktoryzację teoretycznie dowolnej liczby całkowitej w rozsądnym czasie bez względu na liczbę bitów. Odbywa się to poprzez zamianę problemu faktoryzacji na równoważny problem poszukiwania okresu funkcji

$$f(x) = r^x \bmod n \tag{4}$$

zdefiniowanej dla liczb naturalnych. Znalezienie okresu wymaga użycia komputera kwantowego, który wykonuje kwantową transformatę Fouriera. Algorytm Shora został pomyślnie zaimplementowany do faktoryzacji małych liczb, np. 21. Możliwości faktoryzacji silnie zależą od mocy obliczeniowych komputera kwantowego, na razie zbyt ograniczonych do zastosowań praktycznych.

Pomimo tego prowadzone są intensywne prace nad systemami asymetrycznymi, które byłyby odporne na atak komputera kwantowego. Najbardziej obiecujące pod tym względem są [12]:

- schematy podpisu cyfrowego oparte na funkcji skrótu (funkcji haszującej),
- schematy oparte na kodach korekcyjnych,
- algorytmy oparte na kratach teorioliczbowych,
- systemy kryptografii wielomianów wielu zmiennych opartej na kluczu publicznym.

Większość z rozważanych systemów należy do asymetrycznych, gdyż systemy z kluczem prywatnym wykazują wysoką odporność na atak. Ocenia się, że wystarczająca długość klucza zapewniająca bezpieczeństwo w RSPK wynosi 256 bitów [12].

6. Podsumowanie

Pomimo, iż obliczenia kwantowe nie zostały jeszcze wprowadzone na szeroką skalę do zastosowań inżynierskich, postęp w tej dziedzinie każe przypuszczać, że w niedługim czasie przynajmniej częściowo zostaną one wykorzystane praktycznie. Z punktu widzenia bezpieczeństwa RSPK jest to o tyle istotne, że pozwoli zwiększyć ich niezawodność, a przez to rozszerzyć zastosowania w kolejnych dziedzinach produkcji, czy przemysłu. Obecnie uważa się, że najszybciej zostanie zaimplementowana kryptografia kwantowa. Ponieważ do jej implementacji można wykorzystać elementy niewielkich rozmiarów, możliwe będzie użycie go również w trudno dostępnych węzłach RSPK, gdzie znajdują zastosowanie głównie sieci czujnikowe oraz systemy wbudowane niewielkich rozmiarów. Należy też podkreślić, że ze względu na rozmiar zagadnienia, przedstawiony artykuł stanowi jedynie ogólne spojrzenie, pomijając wiele szczegółów technicznych.

7. Literatura

[1] Bilski P., Winiecki W.: Multi-core implementation of the symmetric cryptography algorithms in the measurement system, Measurement, No. 43, 2010, pp. 1049-1060.

[2] Steane A.: Quantum computing. Reports on Progress in Physics (1998), 61(2):117–173.

[3] Shor P.: Algorithms for Quantum Computation: Discrete Logarithms and Factoring, Proceedings 35th Annual Symposium on Foundations of Computer Science (1994), pp. 124-134.

[4] Falahati A., Meshgi H.: Using Quantum Cryptography for Securing Wireless LAN Networks, 2009 International Conference on Signal Processing Systems (2009), pp. 698-701.

[5] Milburn G.: Inżynieria kwantowa, Prószyński i Ska, Warszawa, 1999.

[6] Gielerak R., Sawerwain M.: Sorting of amount of entanglement in quantum states functions implemented for quantum computing simulator, Pomiary, Automatyka, Kontrola (2009), nr 7, pp. 524—527.

[7] Bacon D., van Dam W.: Recent progress in quantum algorithms, Communications of the ACM (2010), Vol. 53, No. 2, pp. 84-93.

[8] Gisin N., Ribordy G., Tittel W. and Zbinden H.: Quantum Cryptography, Reviews of Modern Physics (2002) Vol 74, 145.

[9] Poppe A., Fedrizzi A., Loruenser T., Maurhardt O., Ursin R., Boehm H. R., Peev M., Suda M., Kurtsiefer C., Weinfurter H., Jennewein T., Zeilinger A.: Practical Quantum Key Distribution with Polarization-Entangled Photons, Opt. Express (2004), 12, pp. 3865-3871.

[10] Gisin N., Thew R.T.: Quantum communication technology, Electronics Letters (2010) Vol. 46, No. 14.

[11] Kleinjung T., Aoki K., Franke J., Lenstra A., Thomé E., Bos J., Gaudry P., Kruppa A., Montgomery P., Osvik D. A., te Riele H., Timofeev A. and Zimmermann P.: Factorization of a 768-bit RSA modulus, Cryptology ePrint Archive, 2010, dostępny w http://eprint.iacr.org/cgi-bin/cite.pl?entry=2010/006

[12] Bernstein D.J., Buchmann J., Dahmen E.: Post-Quantum Cryptography, Springer, 2009.

otrzymano / received: 04.08.2010
przyjęto do druku / accepted: 01.10.2010 *artykuł recenzowany*