Zał. nr 4 do ZW 33/2012

WYDZIAŁ INFORMATYKI I ZARZĄDZANIA

KARTA PRZEDMIOTU

Nazwa w języku polskim: Kwantowe systemy kryptograficzne
Nazwa w języku angielskim: Quantum cryptographic systems
Kierunek studiów (jeśli dotyczy): Informatyka
Specjalność (jeśli dotyczy): Bezpieczeństwo i niezawodność systemów informatycznych
Stopień studiów i forma: ~~I~~ / II stopień*, ~~stacjonarna~~ / niestacjonarna*
Rodzaj przedmiotu: obowiązkowy / ~~wybieralny~~ / ~~ogólnouczelniany~~ *
Kod przedmiotu INZ4191
Grupa kursów ~~TAK~~ / NIE*

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	9				18
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	40				60
Forma zaliczenia	Zaliczenie na ocenę				Zaliczenie na ocenę
Dla grupy kursów zaznaczyć kurs końcowy (X)					
Liczba punktów ECTS	1				2
w tym liczba punktów odpowiadająca zajęciom o charakterze praktycznym (P)	0				
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego kontaktu (BK)	0,4				0,8

*niepotrzebne skreślić

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

1. Wiedza i kompetencje z Kryptografii.
2. Wiedza i kompetencje z Bezpieczeństwa sieciowego i internetowego.
3. Wiedza i kompetencje z Rachunku prawdopodobieństwa i statystyki matematycznej.

\

CELE PRZEDMIOTU

C1 Nabycie wiedzy z zakresu podstaw informatyki i kryptografii kwantowej.
C2 Nabycie wiedzy o idei i schematach działania absolutnie bezpiecznych kwantowych kanałów informacyjnych.
C3 Nabycie wiedzy o kwantowej dystrybucji klucza kryptograficznego, bezsplątaniowych i splątaniowych protokołach QKD, destylacja klucza w QKD, uwierzytelnianiu w QKD.
C4 Nabycie wiedzy o współczesnych realizacjach kryptografii kwantowej, przegląd aktualnego stanu rozwoju platform technicznych, projektów badawczych i komercyjnych platform technicznych.
C5 Nabycie wiedzy o rzeczywistym bezpieczeństwie praktycznych realizacji kryptografii kwantowej a także o rodzajach ataków na schematy kryptografii kwantowej.
C6 Nabycie wiedzy z zakresu zaawansowanych metod przetwarzania danych pomiarowych z

systemu oprogramowania id3100 dla platformy kryptograficznej Clavis firmy Id Quantique.

PRZEDMIOTOWE EFEKTY KSZTAŁCENIA

Z zakresu wiedzy student:

PEK_W01 – posiada wiedzę z zakresu podstaw informatyki i kryptografii kwantowej.

PEK_W02 – posiada wiedzę o idei i schematach działania absolutnie bezpiecznych kwantowych kanałów informacyjnych. Zna podstawowe twierdzenia kwantowe – no-cloning, no-deleting, no-broadcasting. Ma wiedzę o splątaniu kwantowym.

PEK_W03 – posiada wiedzę o współczesnych realizacjach kryptografii kwantowej, zna aktualny stan rozwoju platform technicznych, projektów badawczych i komercyjnych platform technicznych na pojedynczych i splątanych fotonach.

PEK_W04 – posiada wiedzę z zakresu zaawansowanych metod przetwarzania danych pomiarowych z systemów oprogramowania i platform technicznych kryptografii kwantowej – DARPA, SECOQC, UQCC, Tokyo QKD Network, IdQuantique, SwissQuantum, MagiQ Technologies, Toshiba.

PEK_W05 – posiada wiedzę z zakresu rzeczywistego bezpieczeństwo praktycznych realizacji kryptografii kwantowej. Zna rodzaje ataków na schematy kryptografii kwantowej.

Z zakresu umiejętności student:

PEK_U01 – potrafi obsługiwać, stosować utrzymywać system oprogramowania id3100 dla kryptograficznej platformy PKI Clavis firmy Id Quantique, a także potrafi prowadzić akwizycję i przetwarzać dane pomiarowe zaawansowanymi metodami statystycznymi oraz metodami data mining.

PEK_U02 - potrafi przedstawić zastosowane metody i uzyskane wyniki przetwarzania danych pomiarowych z platformy kryptograficznej PKI, sporządzić dokumentację z badań, a także przeprowadzić dyskusję na te tematy ze słuchaczami.

Z zakresu kompetencji społecznych student:

PEK_K01 - rozumie korzyści i zagrożenia związane z kryptografią kwantową w zastosowaniach do systemów informatycznych obsługi i automatyzacji procesów społecznych i ekonomicznych. Wy1-Wy7, Se1-Se15

PEK_K02 – umie zespołowo realizować prace badawcze i rozwiązywać problemy.

TREŚCI PROGRAMOWE

Forma zajęć - wykład		**Liczba godzin**
Wy1	Warunkowe bezpieczeństwo kanałów komunikacyjnych opartych o kryptografię klasyczną. Zagrożenie ze strony informatyki klasycznej. Zagrożenie ze strony informatyki kwantowej. Istota kwantowego przetwarzania informacji. Kwantowe algorytmy Shore'a i Grovera. Praktyczna realizacja komputera kwantowego.	1
Wy2	Kryptografia kwantowa jako fundamentalnie bezpieczna metoda transmisji informacji niejawnej. Unikalne własności mechaniki kwantowej w kontekście ochrony informacji. Stany kwantowe i istota pomiaru kwantowego. Podstawowe twierdzenia kwantowe – no-	1

	cloning, no-deleting, no-broadcasting. Splątanie kwantowe.	
Wy3	Kwantowa dystrybucja klucza kryptograficznego. Bezsplątaniowe protokoły QKD. Splątaniowe protokoły QKD. Destylacja klucza w QKD. Uwierzytelnianie.	1
Wy4	Współczesne realizacje kryptografii kwantowej. Technologie realizacji. Pojedyncze fotony. Słabe impulsy laserowe. Splątane fotony.	1
Wy5	Przegląd aktualnego stanu rozwoju platform technicznych. Projekty badawcze. Sieć kwantowa DARPA. Projekt SECOQC. Projekt UQCC oraz Tokyo QKD Network. Projekt SwissQuantum. Dostępność komercyjna platform technicznych IdQuantique, MagiQ Technologies, Toshiba.	1
Wy6	Rzeczywiste bezpieczeństwo praktycznych realizacji kryptografii kwantowej. Rodzaje ataków na schematy kryptografii kwantowej. Denial of Service. Man In The Middle. Weak Measurement. Atak Intercept-resend. Photon number splitting. Beam – splitting. Pozostałe ataki.	1
Wy7	QKD – dystrybucja czy ekspansja tajnego klucza kryptograficznego. Doświadczalne połączenie sieciowe wykorzystujące mechanizmy QKD na PWr w ramach Narodowego Laboratorium Technologii Kwantowych.	1
Wy8	Doświadczalny setup oraz instalacja i opis oprogramowania id3100. Bezpieczna komunikacja z wykorzystaniem demonstracyjnej aplikacji QKD Chat.	1
Wy9	Kolokwium zaliczeniowe.	1
	Suma godzin	**9**

Forma zajęć - ćwiczenia		**Liczba godzin**
Ćw1		
Ćw2		
Ćw3		
Ćw4		
..		
	Suma godzin	

Forma zajęć - laboratorium		**Liczba godzin**
La1		
La2		
La3		
La4		
…		
	Suma godzin	

Forma zajęć - projekt		**Liczba godzin**
Pr1		
Pr2		
Pr3		

Pr4		
…		
	Suma godzin	

Forma zajęć - seminarium		Liczba godzin
Se1	System Id Quantique Clavis. Instalacja oprogramowania id3100. Omówienie tematyki studenckich prac badawczych, sposobu studiowania tematów, przygotowania dokumentacji z badań i prezentacji. Ogólne wiadomości platformie kryptograficznej Clavis firmy Id Quantique oraz o systemie oprogramowania id3100 na tej platformie. Akwizycja tematów studenckich prac badawczych. Id Quantique Clavis - kwantowa dystrybucja klucza na dystansie 5 km w rzeczywistym środowisku testowym. Etap przygotowawczy do uruchamiania i badania platformy	2
Se2	Wymiana klucza z wykorzystaniem protokołu BB84. Wymiana klucza z wykorzystaniem protokołu SARG04. Uruchomienie akwizycji danych z procesu monitorowania i diagnostyki zestawu. Wymiana klucza z wykorzystaniem protokołu SARG04. Uruchomienie akwizycji danych z procesu monitorowania i diagnostyki zestawu. Ekstrakcja danych pomiarowych i analiza możliwości i metod ich przetwarzania.	2
Se3	Analiza działania zestawu doświadczalnego id3100 w rzeczywistym środowisku testowym bez złączek i spawów światłowodowych. Wyniki dla protokołu BB84. Ekstrakcja danych pomiarowych i analiza możliwości i metod ich przetwarzania. Analiza działania zestawu doświadczalnego id3100 w rzeczywistym środowisku testowym bez złączek i spawów światłowodowych. Wyniki dla protokołu SARG04. Ekstrakcja danych pomiarowych i analiza możliwości i metod ich przetwarzania.	2
Se4	Analiza działania zestawu doświadczalnego id3100 w rzeczywistym środowisku testowym z różną ilością złączek i spawów światłowodowych. Wyniki dla protokołu BB84. Ekstrakcja danych pomiarowych i analiza możliwości i metod ich przetwarzania. Analiza działania zestawu doświadczalnego id3100 w rzeczywistym środowisku testowym z różną ilością złączek i spawów światłowodowych. Wyniki dla protokołu SARG04. Ekstrakcja danych pomiarowych i analiza możliwości i metod ich przetwarzania.	2
Se5	Zaawansowana analiza i diagnostyka działania zestawu dla protokołu BB84 bez złączek i spawów światłowodach. Ekstrakcja danych pomiarowych i analiza możliwości i metod ich przetwarzania.	2
Se6	Zaawansowana analiza i diagnostyka działania zestawu dla protokołu BB84 z różną ilością złączek i spawów światłowodach. Ekstrakcja danych pomiarowych i analiza możliwości i metod ich przetwarzania.	2
Se7	Zaawansowana analiza i diagnostyka działania zestawu dla protokołu SARG04 bez złączek i spawów światłowodach. Ekstrakcja danych pomiarowych i analiza możliwości i metod ich przetwarzania.	2
Se8	Zaawansowana analiza i diagnostyka działania zestawu dla protokołu SARG04 z różną ilością złączek i spawów światłowodach. Ekstrakcja danych pomiarowych i analiza możliwości i metod ich przetwarzania.	2
Se9	Raport z badań zestawu dla protokołu BB84 i SARG04. Formułowanie	2

	wniosków z badań dla protokołów BB84 i SARG04 dla różnej ilości złączek i spawów światłowodowych. Dyskusja idei repeterów światłowodowych. Podsumowanie badań.	
	Suma godzin	18

STOSOWANE NARZĘDZIA DYDAKTYCZNE

N1. Wykład tradycyjny oparty o prezentacje multimedialne.
N2. Praca własna studentów – udział w realizacji studenckich prac badawczych
N3. Praca własna – samodzielne studiowanie problematyki wykładu i seminarium oraz prac badawczych z dostępem do platformy kryptograficznej Clavis IdQuantique.
N4. Konsultacje dla studentów.

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW KSZTAŁCENIA

Oceny (F – formująca (w trakcie semestru), P – podsumowująca (na koniec semestru)	Numer efektu kształcenia	Sposób oceny osiągnięcia efektu kształcenia
F1	PEK_U01-PEK_U02	Oceny za wykonanie prac studialnych oraz prezentacje i omówienia.
F2	PEK_U02	Oceny za dokumentację z przestudiowanej problematyki.
P	PEK_W01-PEK_W05, PEK_K01	Kolokwium zaliczeniowe.

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

LITERATURA PODSTAWOWA:

[1] W. Jacak (i in.), *Wstęp do Informatyki i Kryptografii Kwantowej*, Oficyna Wydawnicza Politechniki Wrocławskie, Wrocław 2011.
[2] M. Donderowicz, *Modele kwantowych kryptograficznych kanałów komunikacyjnych z realizacjami na platformach badawczych i w zastosowaniach komercyjnych*, praca magisterska, Politechnika Wrocławska, Wrocław 2012.
[3] W. Jacak, *Aspekty bezpieczeństwa informacji w systemach informatyki klasycznej i kwantowej wraz z analizą możliwości wybranych eksperymentalnych realizacji kwantowego przetwarzania informacji*, praca magisterska, Politechnika Wrocławska, Wrocław 2005.
[4] W. Donderowicz, *Modelowanie bezpiecznych kanałów informacyjnych i projekt kwantowej studialnej platformy badawczej dla wybranych zastosowań informatycznych*, praca magisterska, Poliechnika Wrocławska, Wrocław 2005.
[5] M. Jacak, *Informatyczna implementacja protokołów kryptografii kwantowej na systemach splątanych fotonów(system Clavis II) i splątanych fotonów (system EPR S405 Quelle)*, praca magisterska, Politechnika Wrocławska, Wrocław 2012.
[6] J. Jacak, *Porównanie kwantowego i klasycznego sposobu przechowywania, przetwarzania i zabezpieczania informacji (wybrane aspekty)*, Politechnika Wrocławska, Wrocław 2007.
[7] M. Hirvensalo, *Quantum computing*, Springer-Verlag, Berlin 2001.
[8] *Quantum Distribution System id 3100 Clavis2 User Guide*, Id Quantic, 2012.

[9] *MagiQ Technologies Releases 'Open' Quantum Key Distribution for Researchers Exploring Boundaries of Cryptography*, Business Wire, [Online] MagiQ Technologies, Inc., 2003, opracowanie dostępne pod adresem: http://www.businesswire.com/news/home/20031103005452/en/MagiQ-Technologies-Releases-Open-Quantum-Key-Distribution
[10] A. Pellegrini, V. Bertacco, T. Austin, M.A. Nielsen, I.J. Chuang, *Fault-Based Attack on RSA Authentication*, *Quantum Computation and Quantum Information*, Cambridge, Cambridge University Press, 2000.
[11] Y. Zhao (et al), *Quantum Hacking: Experimental Demonstration of Time-shift Attack Against Practical Quantum-key-distribution Systems*, Phys. Rev. A. 4, Vol. 78, 2008.

LITERATURA UZUPEŁNIAJĄCA:

[1] S. Bellovin, *Security through obscurity*. *Risks Digest*, Forum on Risks to the Public in Computers and Related Systems, ACM Committee on Computers and Public Policy, P.G. Neumann, moderator, Volume 25, Issue 69, 24 May 2009.
[2] A.S. Tanenbaum, *Computer Networks*, Ed. 2nd, Prentice Hall, 2003.
[3] A.S. Godbole, *Data Communications and Networks*, McGraw-Hill Publishing Co. Ltd., 2007.
[4] C. Adams, S. Lloyd, *Understanding Public Key Infrastructure, II*, Pearson Education Inc., 2003.
[5] L.D. Landau, E.M. Lifshic, *Quantum Mechanics*, PWN, Warsaw 1979.

OPIEKUN PRZEDMIOTU (IMIĘ, NAZWISKO, ADRES E-MAIL)

doc. dr inż. Jacek Gruber, 71 320 33 40; jacek.gruber@pwr.wroc.pl

MACIERZ POWIĄZANIA EFEKTÓW KSZTAŁCENIA DLA PRZEDMIOTU
Kwantowe systemy kryptograficzne
Z EFEKTAMI KSZTAŁCENIA NA KIERUNKU Informatyka
I SPECJALNOŚCI Bezpieczeństwo i niezawodność systemów informatycznych

Przedmiotowy efekt kształcenia	Odniesienie przedmiotowego efektu do efektów kształcenia zdefiniowanych dla kierunku studiów i specjalności (o ile dotyczy)**	Cele przedmiotu***	Treści programowe***	Numer narzędzia dydaktycznego***
PEK_W01 (wiedza)	K2INF_W01, K2INF_W02	C1	Wy1	N1,N3-N4
PEK_W02	K2INF_W01, K2INF_W02	C2	Wy2	N1,N3-N4
PEK_W03	K2INF_W01, K2INF_W02, K2INF_W06	C3,C4	Wy4-Wy5, Wy7	N1,N3-N4
PEK_W04	K2INF_W01, K2INF_W02, K2INF_W06	C4	Wy4-Wy5, Wy8	N1,N3-N4
PEK_W05	K2INF_W01, K2INF_W02, K2INF_W06	C4	Wy6	N1,N3-N4
PEK_U01 (umiejętności)	K2INF_U03	C4,C6	Se1-Se9	N2-N4
PEK_U02	K2INF_U06-K2INF_U07	C4,C6	Se1-Se9	N2-N4
PEK_K01 (kompetencje)		C1-C6	Wy1-Wy8, Se1-Se9	N1-N4
PEK_K02		C1-C6	Se1-Se9	N2-N4

** - wpisać symbole kierunkowych/specjalnościowych efektów kształcenia
*** - z tabeli powyżej