

**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~~ / ~~ogólnouniversytecki~~ \***Kod przedmiotu** INZ003966**Grupa kursów** ~~TAK~~ / NIE\*

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	15				30
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				2
w tym liczba punktów ECTS odpowiadająca zajęciom wymagającym bezpośredniego kontaktu (BK)	0,6				1,2

\*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, bezspłatanowych i splecanych 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 bezpieczeństwa 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.	2
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-	2

	cloning, no-deleting, no-broadcasting. Splątanie kwantowe.	
Wy3	Kwantowa dystrybucja klucza kryptograficznego. Bezsplątaniowe protokoły QKD. Splątaniowe protokoły QKD. Destylacja klucza w QKD. Uwierzytelnianie.	2
Wy4	Współczesne realizacje kryptografii kwantowej. Technologie realizacji. Pojedyncze fotony. Słabe impulsy laserowe. Splątane fotony.	2
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.	2
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.	2
Wy7	QKD – dystrybucja czy ekspansja tajnego klucza kryptograficznego. Doświadczalne połączenie sieciowe wykorzystujące mechanizmy QKD na PWR w ramach Narodowego Laboratorium Technologii Kwantowych. Doświadczalny setup oraz instalacja i opis oprogramowania id3100. Bezpieczna komunikacja z wykorzystaniem demonstracyjnej aplikacji QKD Chat.	2
Wy8	Kolokwium zaliczeniowe.	1
	Suma godzin	<b>15</b>

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.	2
Se2	Id Quantique Clavis - kwantowa dystrybucja klucza na dystansie 5 km w rzeczywistym środowisku testowym. Etap przygotowawczy do uruchamiania i badania platformy.	2
Se3	Wymiana klucza z wykorzystaniem protokołu BB84. Wymiana klucza z wykorzystaniem protokołu SARG04. Uruchomienie akwizycji danych z procesu monitorowania i diagnostyki zestawu.	2
Se4	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
Se5	Analiza działania zestawu doświadczalnego id3100 w rzeczywistym środowisku testowym bez złąček i spawów światłowodowych. Wyniki dla protokołu BB84. Ekstrakcja danych pomiarowych i analiza możliwości i metod ich przetwarzania.	2
Se6	Analiza działania zestawu doświadczalnego id3100 w rzeczywistym środowisku testowym bez złąček i spawów światłowodowych. Wyniki dla protokołu SARG04. Ekstrakcja danych pomiarowych i analiza możliwości i metod ich przetwarzania.	2
Se7	Analiza działania zestawu doświadczalnego id3100 w rzeczywistym środowisku testowym z różną ilością złąček i spawów światłowodowych. Wyniki dla protokołu BB84. Ekstrakcja danych pomiarowych i analiza możliwości i metod ich przetwarzania.	2
Se8	Analiza działania zestawu doświadczalnego id3100 w rzeczywistym środowisku testowym z różną ilością złąček i spawów światłowodowych. Wyniki dla protokołu SARG04. Ekstrakcja danych pomiarowych i analiza możliwości i metod ich przetwarzania.	2
Se9	Zaawansowana analiza i diagnostyka działania zestawu dla protokołu BB84 bez złąček i spawów światłowodach. Ekstrakcja danych pomiarowych i analiza możliwości i metod ich przetwarzania.	2
Se10	Zaawansowana analiza i diagnostyka działania zestawu dla protokołu BB84 z różną ilością złąček i spawów światłowodach. Ekstrakcja danych pomiarowych i analiza możliwości i metod ich przetwarzania.	2
Se11	Zaawansowana analiza i diagnostyka działania zestawu dla protokołu SARG04 bez złąček i spawów światłowodach. Ekstrakcja danych pomiarowych i analiza możliwości i metod ich przetwarzania.	2
Se12	Zaawansowana analiza i diagnostyka działania zestawu dla protokołu SARG04 z różną ilością złąček i spawów światłowodach. Ekstrakcja danych pomiarowych i analiza możliwości i metod ich przetwarzania.	2
Se13	Raport z badań zestawu dla protokołu BB84 i SARG04.	2
Se14	Formułowanie wniosków z badań dla protokołów BB84 i SARG04 dla	2

	różnej ilości złączy i spawów światłowodowych. Dyskusja idei repeterów światłowodowych.	
Se15	Podsumowanie badań. Zaliczenia.	2
	Suma godzin	30

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

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

- [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 (IMIE, 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**

<b>Przedmiotowy efekt kształcenia</b>	<b>Odniesienie przedmiotowego efektu do efektów kształcenia zdefiniowanych dla kierunku studiów i specjalności (o ile dotyczy)**</b>	<b>Cele przedmiotu***</b>	<b>Treści programowe***</b>	<b>Numer narzędzia dydaktycznego***</b>
<b>Przedmiotowy efekt kształcenia</b>	<b>Odniesienie przedmiotowego efektu do efektów kształcenia zdefiniowanych dla kierunku studiów i specjalności (o ile dotyczy)**</b>	<b>Cele przedmiotu***</b>	<b>Treści programowe***</b>	<b>Numer narzędzia dydaktycznego***</b>
<b>PEK_W01 (wiedza)</b>	K2INF_W01, K2INF_W02	C1	Wy1	N1,N3-N4
<b>PEK_W02</b>	K2INF_W01, K2INF_W02	C2	Wy2	N1,N3-N4
<b>PEK_W03</b>	K2INF_W01, K2INF_W02, K2INF_W06	C3,C4	Wy4-Wy5, Wy7	N1,N3-N4
<b>PEK_W04</b>	K2INF_W01, K2INF_W02, K2INF_W06	C4	Wy4-Wy5, Wy7	N1,N3-N4
<b>PEK_W05</b>	K2INF_W01, K2INF_W02, K2INF_W06	C4	Wy6	N1,N3-N4
<b>PEK_U01 (umiejętności)</b>	K2INF_U03	C4,C6	Se1-Se14	N2-N4
<b>PEK_U02</b>	K2INF_U06-K2INF_U07	C4,C6	Se1-Se15	N2-N4
<b>PEK_K01 (kompetencje)</b>		C1-C6	Wy1-Wy7, Se1-Se15	N1-N4
<b>PEK_K02</b>		C1-C6	Se1-Se15	N2-N4

\*\* - wpisać symbole kierunkowych/specjalnościowych efektów kształcenia

\*\*\* - z tabeli powyżej