Zał nr 4 do ZW

WYDZIAŁ PODSTAWOWYCH PROBLEMÓW TECHNIKI

KARTA PRZEDMIOTU

Nazwa w języku polskim	:	**Wysoko Wydajne Obliczenia**
Nazwa w języku angielskim	:	**High Performance Computing**
Kierunek studiów	:	Informatyka
Specjalność (jeśli dotyczy)	:	
Stopień studiów i forma	:	magisterskie, stacjonarne
Rodzaj przedmiotu	:	wybieralny
Kod przedmiotu	:	E2_W28
Grupa kursów	:	TAK

	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć zorganizowanych w Uczelni (ZZU)	30		30		
Liczba godzin całkowitego nakładu pracy studenta (CNPS)	75		105		
Forma zaliczenia	zaliczenie				
Dla grupy kursów zaznaczyć kurs końcowy	X				
Liczba punktów ECTS	3		3		
w tym liczba odpowiadająca zajęciom o charakterze praktycznym (P)			3		
w tym liczba punktów odpowiadająca zajęciom wymagającym bezpośredniego kontaktu (BK)	3		3		

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

umiejętność programowania w systemie linux/unix,
znajomość jezyka C oraz C++

CELE PRZEDMIOTU

C1 Poznanie podstawowych metod zrównoleglania obliczeń w wybranych zastosowaniach kryptoanalitycznych

C2 Poznanie przykładowych narzędzi służących do zrównoleglania obliczeń w wybranych zastosowaniach kryptoanalitycznych

PRZEDMIOTOWE EFEKTY KSZTAŁCENIA

Z zakresu wiedzy studenta:

W1 Zna główne ograniczenia prezentowanych na wykładzie metod kryptoanalitycznych

W2 Zna metody zrównoleglania obliczeń właściwe dla klastra obliczeniowego

W3 Zna techniki rozwoju oprogramowania właściwe dla środowiska równoległego

Z zakresu umiejętności studenta:

U1 Potrafi dobrać parametry ataku tak by zoptymalizować wysiłek obliczeniowy dla posiadanych zasobów

U2 Potrafi dostrzec sposoby poprawienia efektywności własnej implementacji (zakładając np. zmianę parametrów systemu)

U3 Potrafi uzasadnić trafność wyboru rozwiązań implementacyjnych powołujac się na odpowiednie źródła

Z zakresu kompetencji społecznych studenta:

K1 Rozumie potrzebę zakładania dodatkowego marginesu bezpieczeństwa w doborze parametrów systemu kryptograficznego

K2 Dostrzega możliwości wykorzystania nabytych umiejętności w innych obszarach

TREŚCI PROGRAMOWE

Forma zajęć - wykłady		
Wy1	Rozproszony system obliczeniowy - możliwe architektury	1h
Wy2	Klaster obliczeniowy - narzędzia administracyjne i biblioteki programistyczne	2h
Wy3	Metoda indeksu obliczania logarytmu dyskretnego w grupie multyplikatywnej ciała skończonego	2h
Wy4	Metoda rho-Pollarda znajdowania logartmu dyskretnego w dowolnej grupie cyklicznej ograniczonego rzędu	2h
Wy5	Zrównoleglenie metody rho-Pollarda	3h
Wy6	Zastosowanie metody rho-Pollarda w algorytmie Pohliga-Hellmana	3h
Wy7	Metoda kangurów obliczania logarytmu dyskretnego dla wykładnika z zadanego przedziału	2h
Wy8	Zrównoleglenie metody kangurów	2h
Wy9	Metoda Lenstry faktoryzacji	2h
Wy10	Tęczowe tablice	2h
Wy11	Metoda sita kwadratowego i sita ciał liczbowych	5h
Wy12	Dedykowane urządzenia przyspieszające sito ciał liczbowych	4h
Forma zajęć - laboratorium		
Lab1	Poznanie środowiska programistycznego dla klastra obliczeniowego	2h
Lab2	Wykorzystanie bibliotek MPI i NTL w prostych zadaniach obliczeniowych	2h
Lab3	Zaimplmentowanie równoległej wersji medody obliczania indeksu	6h
Lab4	Zaimplementowanie metody rho-Pollarda w wersji równoległej	4h
Lab5	Zaimplementowanie metody Pohliga-Hellmana w oparciu o metodę Pollarda	6h
Lab6	Zaimplementowanie metody Lenstry faktoryzacji	4h
Lab7	Zaimplementowanie ataku z wykorzystaniem tęczowych tablic	4h
Lab8	Podsumowanie zajęć laboratoryjnych	2h

STOSOWANE NARZĘDZIA DYDAKTYCZNE

1. Wykład tradycyjny
2. Rozwiązywanie zadań i problemów
3. Rozwiązywanie zadań programistycznych
4. Konsultacje
5. Praca własna studentów

OCENA OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW KSZTAŁCENIA

Oceny	Numer efektu kształcenia	Sposób oceny efektu kształcenia
F1	W1-W3, K1-K2	Egzamin na końcu semestru
F2	U1-U3, K1-K2	Ocena implementacji zadanych algorytmów równoległych
P=40%*F1+60%*F2		

LITERATURA PODSTAWOWA I UZUPEŁNIAJĄCA

1. William Gropp, Ewing Lusk, Rajeev Thakur, Using MPI-2: Advanced Features of the Message-Passing Interface, MIT Press, 1999
2. Paul C. van Oorschot, Michael J. Wiener: Parallel Collision Search with Cryptanalytic Applications. J. Cryptology 12(1): 1-28 (1999)
3. Tim Güneysu, Andy Rupp, Stefan Spitz, Cryptanalytic Time-Memory Tradeoffs on COPACOBANA, GI Jahrestagung 2, Vol. 110GI (2007) , p. 205-209
4. Matthew E. Briggs, An Introduction to the General Number Field Sieve, Masterthesis, 1998

OPIEKUN PRZEDMIOTU

dr Przemysław Kubiak

MACIERZ POWIĄZANIA EFEKTÓW KSZTAŁCENIA DLA PRZEDMIOTU
Wysoko Wydajne Obliczenia
Z EFEKTAMI KSZTAŁCENIA NA KIERUNKU INFORMATYKA

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**
W1	K2_W02	C1	Wy1-Wy12	1 4 5
W2	K2_W01	C1	Wy1-Wy12	1 4 5
W3	K2_W09	C1	Wy1-Wy12	1 4 5
U1	K2_U08 K2_U10 K2_U14	C1	Lab1-Lab8	2 3 4 5
U2	K2_U18 K2_U19 K2_U21	C1	Lab1-Lab8	2 3 4 5
U3	K2_U01 K2_U07 K2_U16	C1	Lab1-Lab8	2 3 4 5
K1	K2_K12	C1 C2	Wy1-Wy12 Lab1-Lab8	1 2 3 4 5
K2	K2_K01 K2_K12 K2_K13	C1 C2	Wy1-Wy12 Lab1-Lab8	1 2 3 4 5