Faculty of Fundamental Problems of Technology

COURSE CARD

Name in polish	:	**Wysoko Wydajne Obliczenia**
Name in english	:	**High Performance Computing**
Field of study	:	Computer Science
Specialty (if applicable)	:	
Undergraduate degree and form of	:	masters, stationary
Type of course	:	optional
Course code	:	`E2_W28`
Group rate	:	Yes

	Lectures	Exercides	Laboratory	Project	Seminar
Number of classes held in schools (ZZU)	30		30		
The total number of hours of student workload (CNPS)	75		105		
Assesment	pass				
For a group of courses final course mark	X				
Number of ECTS credits	3		3		
including the number of points corresponding to the classes of practical (P)			3		
including the number of points corresponding occupations requiring direct contact (BK)	3		3		

PREREQUISITES FOR KNOWLEDGE, SKILLS AND OTHER POWERS

ability to program in linux / unix operating system, knowledge of C and C++ programming language

COURSE OBJECTIVES

C1 Providing basic methods for parallelization of computations in some cryptanalytic applications.

C2 Providing knowledge of exemplary tools for parallelization of cryptanalytic computations.

COURSE LEARNING OUTCOMES

The scope of the student's knowledge:

W1 Knows the main limitations of the cryptanalytic methods presented.

W2 Knows the parallelization methods specific to cluster computing.

W3 Knows the art software development suitable for parallel environment.

The student skills:

U1 Is able to adjust parameters of the attack in such a way that the computational effort is (nearly) optimal for available resources.

U2 Is able to see ways of improving effectiveness of her/his own implementation (in case of a change of system parameters).

U3 Relying on appropriate sources the student can justify the relevance of the solutions implemented.

The student's social competence:

K1 Understands the need for an additional security margin in the selection of parameters of a cryptographic algorithm.

K2 Sees the possibility of using the acquired skills in other areas.

COURSE CONTENT

Type of classes - lectures		
Wy1	Distributed computing system - possible architectures.	1h
Wy2	A computer cluster - administrative tools and programming libraries.	2h
Wy3	Index calculus method for computing discrete logarithms in a multiplicative group of a finite field.	2h
Wy4	Pollard rho-method.	2h
Wy5	Parallelization of the Pollard rho-method.	3h
Wy6	Application of the Pollard rho-method in the Pohlig-Hellman algorithm.	3h
Wy7	Kangaroo method for computing a discrete logarithm that belongs to some known interval.	2h
Wy8	Parallelization of the kangaroo method.	2h
Wy9	Lenstra's elliptic curve factorization algorithm.	2h
Wy10	Rainbow tables.	2h
Wy11	Quadratic sieve and the number field sieve.	5h
Wy12	Dedicated hardware designed for factorization.	4h

Type of classes - laboratory		
Lab1	Programming environment for a computer cluster.	2h
Lab2	MPI and NTL libraries in basic parallelization tasks.	2h
Lab3	Implementation of a parallel version of the index calculus method.	6h
Lab4	Implementation of a parallel version of the Pollard rho method.	4h
Lab5	Implementation of a parallel version of the Pohlig-Hellman algorithm with the Pollard rho method as a component.	6h
Lab6	Implementation of Lenstra's elliptic curve factorization algorithm.	4h
Lab7	Implementation of an attack based on rainbow tables.	4h
Lab8	Summary of the laboratory classes.	2h

Applied learning tools

1. Traditional lecture
2. Solving tasks and problems
3. Solving programming tasks
4. Consultation
5. Self-study students

EVALUATION OF THE EFFECTS OF EDUCATION ACHIEVEMENTS

Value	Number of training effect	Way to evaluate the effect of education
F1	W1-W3, K1-K2	an exam at the end of the semester
F2	U1-U3, K1-K2	Evaluation of implementation of algorithms specified during the classes.
P=40%*F1+60%*F2		

BASIC AND ADDITIONAL READING

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

SUPERVISOR OF COURSE

dr Przemysław Kubiak

RELATIONSHIP MATRIX EFFECTS OF EDUCATION FOR THE COURSE
High Performance Computing
WITH EFFECTS OF EDUCATION ON THE DIRECTION OF COMPUTER SCIENCE

Course training effect	Reference to the effect of the learning outcomes defined for the field of study and specialization (if applicable)	Objectives of the course**	The contents of the course**	Number of teaching tools**
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_B K2_U10 K2_U14	C1	Lab1-Lab8	2 3 4 5
U2	K2_U18_B K2_U19_B K2_U21_B	C1	Lab1-Lab8	2 3 4 5
U3	K2_U01_B 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_B K2_K12 K2_K13	C1 C2	Wy1-Wy12 Lab1-Lab8	1 2 3 4 5