

## **Kiraz, Mehmet Sabir**

Department of Mathematics and Computer Science  
Eindhoven University of Technology  
P.O. Box 513 5600 MB Eindhoven  
The Netherlands

**E-mail:** [kiraz\\_mehmet@hotmail.com](mailto:kiraz_mehmet@hotmail.com)

**Web:** <http://www.win.tue.nl/~mkiraz/>

**Mobile:** +31 (0) 62 806 85 31

### **Career objectives:**

- To make further study in a number of core areas in Mathematics.
- To be a professional in Cryptography and gain practical and academic experience in Cryptography.

### **Educational Status:**

**2004 March / 2008 March (Expected):** Ph.D. Research in Cryptography from Computer Science and Mathematics in Technical University of Eindhoven, Eindhoven, The Netherlands

- Two-Party computation, Zero-Knowledge Proofs, Commitments
- Verification of Cryptographic protocols
- Program analysis

**2002 September/2003 October:** Master of Computer Science from Max Planck Institut Für Informatik and University of Saarland, Saarbrücken, Germany.

- Taken courses on Information Retrieval and Data Mining, Computer Architecture, Data Structure and Algorithms, Approximation Algorithms, Randomized Algorithms, Differential Equations in Image Processing and Computer Vision, Security, Selected areas in Cryptography, Theory of Complex Network, Security
- Developed, with Java, a search engine similar to Google,
- Implemented, with Object CAML, part of my Master's thesis.

### **Post-graduate Experience:**

#### **- Computer Architecture:**

Duration: October 2002- Feb. 2003

Guidance: Prof. Dr. Wolfgang J.Paul

Computer Science, Saarland University

Grade: 1.0 (A+)

This course was to understand the schematics of a processor with superpipelining, delayed branch, forwarding, hardware interlock, speculative execution, caches, nested precise interrupts and out of order execution. The correctness of most constructions is also done through formal verification.

– **Data structures and Algorithms:**

Duration: October 2002- Feb. 2003

Guidance: Prof. Dr. Raimund Seidel

Computer Science, Saarland University

– **Randomized Algorithms:**

Duration: October 2002- Feb. 2003

Guidance: Dr. Peter Sanders, Dr. Ernst Althaus

Max Planck Research Institute for Computer Science

Many algorithmic problems have a simple, elegant and efficient solution if one allows randomization, i.e., decisions of the algorithm are not only based on the input but also on the value of some random event. This course teaches techniques for the design and analysis of randomized algorithms.

– **Approximation Algorithms(Seminar):**

Duration: October 2002- Feb. 2003

Guidance: Dr. Friedrich Eisenbrand, Dr. Stefan Funke,

Dr. Piotr Krysta

Max Planck Research Institute for Computer Science

Grade: 2.0 (B+)

Study of Set Cover, Steiner Tree and TSP, Multiway Cut & k-cut, k-center, Feedback Vertex set, Shortest Superstring, Knapsack, Bin packing, Minimum Makespan Scheduling, Euclidean TSP, A careful introduction to LP duality, Set Cover via Dual Fitting/Rounding/Primal-Dual Schema, Max SAT, Scheduling on unrelated parallel Machines, Multi Cut, Steiner Forest, Steiner

Network, Facility Location, k-Median, Semidefinite Programming, Shortest Vector, Hardness of Approximation.

- **Information Retrieval and Data Mining:**

Duration: October 2002- Feb. 2003

Guidance: Prof. Dr. Gerhard Weikum

Computer Science, Saarland University

Grade: 2.0 (B+)

Information Retrieval and Data Mining are the technologies for searching, analyzing and automatically organizing text documents, multimedia documents, and structured or semi-structured data. It covers mathematical models and algorithms on which search engines for the Web and Intranets as well as data analysis tools are based.

- **Selected Areas in Cryptography:**

Duration: Apr. 2003- July. 2003

Guidance: Dr. Ammar Alkassar

Computer Science, Saarland University

Grade: 1.0 (A+)

Study of some of the techniques of cryptography such as secret sharing scheme, Byzantine Agreement, Commitments, Oblivious Transfer, Zero Knowledge Proofs, Coin Flipping

- **Security:**

Duration: Apr. 2003- July. 2003

Guidance: Dr. Dieter Hutter

Dr. Werner Stephen

German research center for Artificial Intelligence(DFKI)

Study of various security techniques like cryptographic approaches, Asymmetric Encryption (RSA, Diffie Hellman, Al-Gamal), Symmetric Encryption (Block and stream cipher), Privacy, Integrity, Accessibility, Security Protocols, approaches of Network Security (Firewalls, IDS, Mixes etc.), Security Engineering (Threat Analysis, Formalization of Security Aspects) and Applications.

- **Master Thesis:**

Topic: Formalization and Verification of Informal Security Protocol Descriptions.

Guidance: Dr. Bruno Blanchet

Head of Static Analysis Group, MPI

The thesis consists of theoretical study of protocols in the presence of an adversary. Translation into Horn clauses for the use of Protocol Verifier developed by MPI using Ocaml as a programming language.

**1996 September/2000 August** : B.Sc. in Mathematics, Middle East Technical University, Ankara/Turkey. GPA: 3.45 (out of 4.00).

**Awards & Honors:**

- Full scholarship for Master of Computer Sc., Max Planck Research Institute for Informatik 2002/2003 which were granted to only 16 students from all over the world.
- Fellowship for B.Sc., Middle East Technical University 1996/2000
- Full scholarship of Government, Mersin Anatolian Teacher's High School 1992/1996

**Work Experience:**

**1) 2001 August - 2002 October:** YAPI KREDI BANK, Address: Istanbul, Turkey  
Technology Department, Position: System Analyst/Senior Mainframe Programmer  
(Analysis, Design, and Programming)

- Used COBOL for mainframe (for interface and batch) and Java for Internet banking.
- Developing batch and on-line programs using mainly Cobol,VS Cobol II

PLI,JCL , CICS , DB2 and SQL on IBM OS 390 and MVS mainframe. Also the secondary tools like file aid, Expediter (Debugger), Endavor (Compiler) in development process are also used.

- Making a front analysis before either starting a new project or a making a corrective maintenance, considering the feedbacks from end-user groups.
- Making unit test and the integrity test of the software in test environment considering the test scenarios, I prepared. For major projects end-user groups from several branches of the banks are also called to make functional and integration tests.
- Moving the programs, copybooks, jcls, copylibs to the production Host environment using Endeavor tool.
- Being in charge with the batch process ,in case of an error , fixing the error and re-executing the job that is disturbed.

**2) 2000 july - 2001 August** : PAMUKBANK T.A.S. Address: Istanbul, Turkey IT System Development Department, Position: System Analyst/ Mainframe Programmer(Analysis, Design, Programming, and Test)

- Change and modify the appearance and functionality of internet branch of Pamukbank. Skills used: HTML, ASP, JavaScript, Java, Visual Studio,
- Dialog online banking using COBOL with CICS as programming language,
- Participated in the following projects: a) Credit-Risk Analysing, b) Risk Centralization, c) Mutual Funds, d) EFT, f) Internal Money Transfer,
- Experienced in developing system design requirements and specifications from marketing or user demands, in wide range software, development tools, methodologies and familiar with a variety of software development tools.

### **Computer Skills:**

**Programming Languages:** Objective CAML; Prolog; JAVA; PLI (MVS/VSE); COBOL; VS COBOL II; IBM Mainframe; CICS; DB2; MVS environment (TSO/ISPF AND JCL); IBM OS-390 mainframe - expert; Visual Age Generator (VG); Pascal; Fortran; Intermediate in Visual Basic; EastmenSw.

**Operating Systems:** Linux, MS-DOS, Windows 95/98/NT4/2000/XP

**Application Programs:** MS Office (Word, Excel, Access), Adobe Photoshop, MATLAB

**Database Applications:** DB2 (MVS/VSE), SQL Server

**Others:** HTML; LATEX; ASP; Frontpage; JavaScript; lex; Yacc

### **Seminars and Certificates:**

- 3 months of training about Banking and Economics.
- 3 weeks of training about CARDPAC credit card management system by Pamukbank Credit Card IT staff.
- 1 month of training about XML, JavaScript, HTML, JCL by Pamukbank's IT staff.
- Training about VS COBOL II and DB2 given by IBM.

### **Languages:**

Turkish (Native Speaker)

Fluent Written and Spoken English

Intermediate in Dutch (read, write, spoken)

Beginner in German (read, write, spoken)

### **Hobbies:**

Reading in computer sciences, playing strategic computer games, travelling abroad, listening to club music, clubbing, watching and playing basketball, soccer, table tennis, billiard and bowling, and attending friendly meetings.

### **Personal Information:**

**Nationality:** Turkish

**Date of Birth:** 02.10.1977 **Marital Status:** Married

### **References:**

1. Dr. Bruno Blanchet  
Max Planck Research Institute  
Saarbrücken, Germany

email: [blanchet@mpi-sb.mpg.de](mailto:blanchet@mpi-sb.mpg.de)

**2.**Prof. Dr. Wolfgang J. Paul

Department of Computer Science

Saarland University(Germany)

email: [wjp@cs.uni-sb.de](mailto:wjp@cs.uni-sb.de)

**3.**Dr.Ammar Alkassar

Department of Computer Science

Saarland University(Germany)

email: [alkassar@cs.uni-sb.de](mailto:alkassar@cs.uni-sb.de)

**4.**Umit Altinay

Head of Technology Develeopment Center

Yapi Kredi Bank, Istanbul, Turkey

email: [ualtinay@ykb.com](mailto:ualtinay@ykb.com)