Rosario Gennaro

Laboratory for Computer Science, NE43-344
545 Technology Square, MIT
Cambridge, MA 02139
(617) 253-6259 Fax: (617)253-3480

80 Rutland St.
Boston, MA 02118
(617) 859-5832
E-mail: rosario@lcs.mit.edu

OBJECTIVE: A research position in Computer and Network Security, Cryptography or a related field starting the summer or the fall of 1996

PROFESSIONAL INTERESTS: Computer and Network Security, Cryptography and Cryptanalysis.
Theoretical Computer Science: Distributed Computation, Algorithms and Complexity Theory, Machine Learning, Computational Geometry, Computer Algebra, Logic.

EDUCATION:

Massachusetts Institute of Technology, 1990–present. Cambridge, MA
Ph.D. in Computer Science expected, June, 1996. Thesis work under Prof. Silvio Micali. Tentative thesis title: *Theory and Practice of Verifiable Secret Sharing.* The work will introduce formal treatment of fault-tolerant secret sharing protocols and their extension to secure distributed computation in a variety of models. Applications to group signature schemes and key escrow will also be presented.

M.S. in Computer Science, February 1993. Thesis work under Prof. Silvio Micali. Thesis title: *On the definition and properties of Zero-Knowledge Arguments.* The work provides a new formal definition for an interesting variant of zero-knowledge protocols and presents various applications.

Università di Catania, 1985-1989. Catania, Italy
Laurea in Matematica (Bachelor's degree in Mathematics), *summa cum laude.* Thesis on *Computational Geometry: Algorithms and Applications.*

Università di Perugia, Summer 1989. Perugia, Italy
Summer school for outstanding italian mathematics majors. Attended advanced classes in Numerical Analysis and Theory of Computer Programming.

WORK EXPERIENCE:

MIT Laboratory for Computer Science, 1990-present Cambridge, MA
Research Assistant. Investigated the subject of secure protocols in various different models of distributed computation. Research focused on the use of zero-knowledge protocols for the achievement of the composition and independence properties in secure protocols (see publications.)

Massachusetts Institute of Technology, Summer and Fall 1995. Cambridge, MA
Teaching assistant for *Computer and Network Security*, a senior class for computer science majors. The class covered practical security issues and state-of-the-art technology in the design of computer systems and network protocols. Closely collaborated with the instructor to create this newly offered course. Summer work included course preparation and research on the topics to be covered. Once the semester started, gave lectures, held office hours and tutorials, prepared and graded problem sets and quizzes.

Massachusetts Institute of Technology, Fall 1992–93–94 and Spring 1995. Cambridge, MA
Teaching assistant. Assisted instructor for *Introduction to Algorithms*, both the undergraduate and graduate version of the class. Taught weekly recitations and some lectures. Held office hours and tutorials. Prepared and graded problem sets and quizzes. Received high marks from students in final evaluation.

Università di Catania, 1989-1990 Catania, Italy
Research assistant. Worked on a team developing an automated theorem prover for Euclidean geometry.

BACKGROUND INFORMATION:

Citizenship: Italian. F-1 Visa in the U.S.

Programming experience: Pascal. Some experience in Lisp, Scheme and PROLOG.

Language skills: Italian (native), English (fluent).

AWARDS: **Fellowship from Opera Universitaria di Catania**, 1988.
Prize for best Science student at the Università di Catania.

PUBLICATIONS: See attached list.

REFERENCES: Available upon request.

Rosario Gennaro

List of Publications

CRYPTOGRAPHY:

Verifiable Secret Sharing as Secure Computation, with S. Micali. Proceedings of EUROCRYPT 1995. Also as MIT Laboratory for Computer Science Technical Memo no.502.

Achieving Independence Efficiently and Securely. Proceedings of 1995 ACM Symposium on Principles of Distributed Computing Systems (PODC 1995). Also as MIT Laboratory for Computer Science Technical Memo no.515.

A Receipt–free Election Scheme Tolerating a Dynamic Coercer (with Applications to Key Escrow). Submitted to EUROCRYPT 1996.

Proactive Threshold DSS Signatures, with S. Jarecki, H. Krawczyk, T. Rabin. Submitted to EUROCRYPT 1996.

Partial Cryptanalysis of Koyama's Eurocrypt'95 Scheme, with A. Shamir. Submitted to EUROCRYPT 1996.

Multi-Verifier Interactive Proofs, with J. Kilian. Submitted to EUROCRYPT 1996.

Robust Sharing of RSA Functions, with S. Jarecki, H. Krawczyk, T. Rabin. In preparation, to be submitted to CRYPTO 1996.

Secure Multiparty Computation without Receipts. In preparation, to be submitted to the 1996 ACM Symposium on Theory of Computing (STOC 1996.)

LEARNING AND AI:

On Learning from Noisy or Incomplete Examples, with S. Decatur, Proceedings of the 1995 ACM Conference on Computational Learning Theory (COLT 1995.)

Probabilistic Verification of Elementary Geometry Statements, with G. Carrà-Ferro and G. Gallo. Proceedings of the 1995 IMACS Conference on the Applications of Computer Algebra.

PAC-Learning PROLOG Clauses with or without Errors, MIT Laboratory for Computer Science Technical Memo no.500.