ROSARIO GENNARO

Curriculum Vitae (11/95)

MIT Laboratory for Computer Science
545 Technology Square, Room 344
Cambridge, MA 02139
Phone: (617) 253-6259
Fax: (617) 253-3480
rosario@theory.lcs.mit.edu

80 Rutland Street
Apartment #2
Boston, MA 02118
Phone: (617) 859-5832

Research Interests

My main research interests are Cryptology and Computer and Network Security, which I intend to develop both at the theoretical and applied level. In particular I am interested in working on the security issues connected with the growth of Internet. I am also interested in other computer science topics such as algorithms, computational complexity, machine learning.

Education

Massachusetts Institute of Technology, Cambridge MA.
Doctor of Philosophy in Electrical Engineering and Computer Science, expected June 1996.
Thesis Title: *Theory and Practice of Verifiable Secret Sharing.*
Supervisor: Professor Silvio Micali.
Minor: Communication and Information Theory.

Massachusetts Institute of Technology, Cambridge MA.
Master of Science in Electrical Engineering and Computer Science, February 1993.
Thesis Title: *On the Definition and Properties of Zero-Knowledge Arguments.*
Supervisor: Professor Silvio Micali.

Università di Catania, Italy.
Laurea in Matematica, *summa cum laude*, November 1989.
Award for Best Science Student in 1988.

Professional Experience

MIT Laboratory for Computer Science.
1990/present: Research Assistant in the Theory of Computation Group. Worked on cryptography and distributed computation. Supervisor Prof. Silvio Micali.

MIT Department of Electrical Engineering and Computer Science
Teaching Assistant for the following courses:

- *Summer and Fall 1995:* Computer and Network Security, a newly offered course in the Department, for seniors and first-year graduate students. Summer work included research on the topics to be covered and preparation of the curriculum. Supervisor: Professor Ronald Rivest.
- *Spring 1995:* Theory of Algorithms, a graduate course. Supervisor: Professor Silvio Micali.
- *Fall 1992/93/94:* Introduction to Algorithms, an undergraduate course. Supervisors: Profs. Shafi Goldwasser (92), Bonnie Berger (93) and Silvio Micali (94).

Taught weekly recitations, and occasionally gave lectures. Designed and graded exams, homework assignments and implementation projects. Met with students regularly to discuss topics of lectures and assist them with homework and research projects. Supervised several student graders.

Università di Catania, Italy.
6/1989–6/1990: Research Assistant. Worked on a team developing an automated theorem prover for Elementary Geometry.

Publications

Refereed Conference Papers

1. R. Gennaro and S. Micali, *Verifiable Secret Sharing as Secure Computation.* Proceedings of EUROCRYPT'95, pp.168–182, Lecture Notes in Computer Science no.921, Springer–Verlag.
2. R. Gennaro, *Achieving Independence Efficiently and Securely.* Proceedings of the Fourteenth Annual ACM Symposium on Principles of Distributed Computation, 1995, pp.130–136, ACM Press. Invited for the special issue of the Journal of Distributed Computing dedicated to the conference.
3. S. Decatur and R. Gennaro, *On Learning from Noisy or Incomplete Examples.* Proceedings of the Eighth Annual Conference on Computational Learning Theory, 1995, pp.353–360, ACM Press.
4. G. Carrà–Ferro, G. Gallo and R. Gennaro, *Probabilistic Verification of Elementary Geometry Statements*, Proceedings of the 1995 IMACS Conference on the Applications of Computer Algebra.

Submitted Papers

5. R. Gennaro, *A Receipt–Free Election Scheme tolerating a Dynamic Coercer (with applications to Key Escrow).* Submitted to EUROCRYPT'96.

6. R. Gennaro and A. Shamir, *Partial Cryptanalysis of Koyama's encryption scheme.* Submitted to EUROCRYPT'96.

7. R. Gennaro, S. Jarecki, H. Krawczyk and T. Rabin, *Robust Threshold DSS Signatures.* Submitted to EUROCRYPT'96.

8. R. Gennaro and J. Kilian, *Multi–Verifier Proofs.* Submitted to EUROCRYPT'96.

9. R. Gennaro, *Secure Multiparty Computation without Receipts.* Submitted to the 1996 ACM Symposium on Theory of Computing.

Work in progress

10. R. Gennaro and S. Micali, *Verifiable Secret Sharing and Secure Computation over general access structures.* Unpublished manuscript, 1995.

11. R. Gennaro, S. Jarecki, H. Krawczyk and T. Rabin, *Robust and Efficient Sharing of RSA Functions.* Unpublished manuscript, 1995.

Technical Reports

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

Invited Lectures

1. *Robust and Efficient Sharing of RSA Functions.* Presented at the MIT Laboratory for Computer Science, December 1995.

2. *A Receipt–Free Election Scheme tolerating a Dynamic Coercer (with applications to Key Escrow).* Presented at AT&T Bell Labs, Murray Hill and MIT Laboratory for Computer Science, November 1995.

3. *Achieving Independence Efficiently and Securely.* Presented at the Fourteenth Annual Symposium on Principles of Distributed Computation, Ottawa, August 1995.

4. *Verifiable Secret Sharing as Secure Computation.* Presented at EUROCRYPT'95, Saint-Malo, May 1995. Also at Università di Catania, June 1995.

5. *On Learning from Noisy or Incomplete Examples.* Presented at Università di Catania, December 1994.

References

1. **Professor Silvio Micali.**
MIT Laboratory for Computer Science
545 Technology Square,
Cambridge, MA 02139.
Telephone: (617) 253-5949,
Fax: (617) 253-3480
My Ph.D. and M.S. thesis supervisor. Leading researcher in cryptography and theoretical computer science.

2. **Professor Shafi Goldwasser.**
MIT Laboratory for Computer Science
545 Technology Square,
Cambridge, MA 02139.
Telephone: (617) 253-5914,
Fax: (617) 253-3480
Email: `shafi@theory.lcs.mit.edu`
Member of my Ph.D. thesis committee. Also I assisted her in teaching "Introduction to Algorithms". Leading researcher in theoretical computer science, cryptography, complexity theory.

3. **Professor Ronald L. Rivest.**
MIT Laboratory for Computer Science
545 Technology Square,
Cambridge, MA 02139.
Telephone: (617) 253-5880,
Fax: (617) 253-3480
Email: `rivest@theory.lcs.mit.edu`
I assisted him in designing and teaching "Computer and Network Security". Leading researcher in theoretical computer science, cryptography, machine learning. Associate Director of MIT Laboratory for Computer Science.

Summary of Previous Research

In the following the numbers refer to the list of papers in page 2.

Theory and Practice of Verifiable Secret Sharing

My Ph.D. thesis studies problems in secure distributed computation. In a Secret Sharing protocol a dealer shares a secret among n servers so that only subsets of $t+1$ or more can reconstruct the secret. A Verifiable Secret Sharing (VSS) protocol adds resilience to the above task. That is, at the end of the sharing phase, the servers have a guarantee that such a secret has been shared and that when they get together they will indeed reconstruct it, no matter what at most t corrupted servers may do. VSS protocols have been shown in the past to be of crucial importance in the design of secure cryptographic protocols.

I first address the problem of formally defining what VSS is. Despite the centrality and the maturity of this concept, I advocate that a stronger and better definition of a VSS is needed. Indeed I show that informal definitions, similar to the one given above, all suffer from a common problem. The VSS protocols that satisfy them, do not enjoy a desirable reducibility property. That is, such VSS protocols, although secure in and by themselves, fail to remain so when used as subroutines inside much larger protocols. I present a new formal definition for VSS that provably enjoys such reducibility property. I also devise VSS protocols that satisfy the new definition. These results appeared in [1].

I also generalize the notion of VSS. Traditionally VSS protocols have threshold security. That is they maintain their security until a given threshold of the servers in the network correctly performs the protocol. For example, above we described a VSS with threshold t. However, implicit in the notion of threshold security is the idea that all servers are identical and that an adversary can corrupt server A with the same effort that it would take to corrupt server B. This is, generally, not the case. Different servers may have different security levels and corrupting one may be easier than breaking into another one. I adapt the notion of access structure to VSS protocols. An access structure is a family of subsets of the servers that we call the authorized subsets. When the dealer shares the secret, only authorized subsets of players can reconstruct it later. Protocols for sharing a secret with general access structures are known in the literature, but they are not fault-tolerant. We construct new resilient VSS protocols for the access structure model. However since the notion of threshold is missing, a legitimate question is: what kind of adversaries will be tolerated by the protocols? Above we knew that adversaries who corrupt at most t players were tolerable. In order to overcome this problem I define the notion of admissible adversary, which is an adversary that by corrupting servers does not destroy the integrity of the access structure (see [10].)

The third part of the thesis presents applications of VSS to the practical issue of robust shared signature schemes. Although maintaining rigorous formal treatment, special emphasis is given to the efficiency of the protocols. Shared signatures allow a group of servers to sign a document with a secret key that is shared among them. I present efficient threshold signature schemes for the Digital Signature Standard and the RSA Signature Algorithm. The protocols are fully robust, that is they tolerate the presence of a threshold of malicious servers who may try to impede the signature process (see [7] and [11].)

Simultaneous Broadcast

Simultaneous Broadcast is a fundamental tool to achieve security in fault tolerant distributed computing. It allows n processes in a loosely synchronized network, to simultaneously announce independent values, in spite of the possible correlation between messages.

In [2] I present the first constant round protocol to perform this task under general complexity assumptions. Previous solutions were all $O(\log n)$ rounds. In the process I develop a new and stronger formal definition for this problem.

Uncoercibility in Cryptographic Protocols

Recently the cryptographic community has given a lot of attention to the problem of coercion in cryptographic protocols. Traditional encryptions protect the privacy of the users, but do not protect them from a coercer who may try to force them to reveal information. For example in electronic elections, besides secrecy of the casted votes, it is also necessary that voters be able to prove to a coercer that they casted either vote. Cryptographic protocols with such property are usually referred as Uncoercible or receipt–free.

In [5] I present a simple receipt-free election protocol that tolerates a dynamic coercer who actively cooperates with some of the voting authorities. Previous works instead assumed that the coercer was a static entity who had just listened only to the public transcript of the protocol.

I also investigate the notion of uncoercibility for generic secure multiparty computation protocols in [9]. I formally define receipt–freeness and compare this notion to the traditional notion of security. I also prove that receipt-free protocols are impossible to obtain without some physical mean of hiding information.

Cryptanalysis

In [6] I present a partial attack on the encryption scheme presented by Koyama at EUROCRYPT'95. Although claimed to be as secure as RSA, the scheme leaks partial information about the plaintext that is not leaked by regular RSA encryptions. Also I show how this partial information can be used to completely decrypt the ciphertext when some additional algebraic information about the plaintext is given.

Learning and AI

In [3] I investigate learnability in the PAC model when the data used for learning is either corrupted or incomplete. The main result is to show learnability of a large class of Boolean predicates when random noise is present in both the attributes and the classification labels. These are the first PAC models to capture a learning environment in which *all* training data, attributes and labels, may be corrupted by a random process. Extensions of these results to the case of restricted classes of PROLOG clauses are presented in [12].

In [4] I present a probabilistic procedure to estimate the probability of a given geometric statement to be true in general once it has been proven to hold for a certain number of randomly chosen examples. Applications to motion planning and robotics are also discussed.

Future Research Directions

I will continue working on security issues in distributed computation. It is a very exciting time to do research in this area. The explosive growth in the number of users and applications of Internet provides the ideal application field for a whole body of theory developed by the cryptographic community in the past two decades.

The main challenge that I foresee is to abandon the classical notion of threshold security and move towards more flexible security policies based on general access structures. Nowadays the robustness of cryptographic protocol is analyzed under the assumption that only a threshold (like less than half or a third) of the participants might behave incorrectly. As I argued in my doctoral thesis, this may not be sufficient. It is time to begin designing and analyzing protocols from a more general point of view. The role of different players in a given cryptographic protocol is usually not interchangeable: some servers are more important than others, some are more secure, others are computationally more efficient and so on. I intend to make all these issues relevant in the design and implementation of cryptographic protocols.

A typical example is the case of shared signature schemes. In my thesis I presented robust, i.e. able to tolerate malicious parties, protocols for the threshold scenario, in which a signature is produced if a threshold of shareholders cooperate. However one might want to implement more versatile policies: for example a bank may require either the president and half of the board of directors or two thirds of the board alone to cooperate to sign transactions. The challenge is to devise efficient protocols for such tasks and it involves interesting mathematical problems to be analyzed and solved.

The shared signature case is just an example. It is however very important for practical applications. Robust shared signature schemes (either in the threshold or in the access structure model) are very relevant for the implementation of a versatile and robust public–key infrastructure (PKI) for the Internet. The role of the PKI will be to certify users' public keys. Having a shared certification procedure will eliminate the single point of failure created by a single certification authority and protect users against possible security breaches in the PKI servers. I plan to work on this and similar applications of my work on secure shared signatures.

I will also explore other areas of secure distributed computation. I am particularly interested in investigating the notion of uncoercibility for cryptographic protocols. Although electronic elections remain the most important application for this notion, I strongly suspect that receipt–free protocols are going to be needed in other security scenarios.

Probably the most important application area in the near future is to get the Internet ready for the advent of the electronic commerce era. There are formidable challenges in this area especially in trying to transform the theoretical cryptographic tools we are in possess of into efficient solutions that can be implemented and used in practice. I intend to be actively involved in this effort.

Teaching Statement

During my graduate years at MIT, I have aided in teaching courses at the graduate and undergraduate level. During Summer and Fall 1995 I worked with Professor Ronald Rivest on preparing and teaching "Computer and Network Security" a newly offered course for seniors and first–year graduate students. I also assisted Professor Silvio Micali in teaching "Theory of Algorithms", a graduate course, in the Spring of 1995. During Fall 1992/93/94 I was teaching assistant for Professors Shafi Goldwasser, Bonnie Berger and Silvio Micali, respectively, for the undergraduate class "Introduction to Algorithms".

I was responsible for leading recitation classes, designing and grading exams and homework assignments, and offering individual assistance to students. Their evaluation of my teaching was always extremely positive. Many students said I motivated and helped them greatly in mastering the material. All the professors I worked with, acknowledged my large impact on developing the students' interests and skills and creating research opportunities for them.

I was responsible for the supervision of several student graders. On various occasions I taught the lectures. The professors acknowledged my ability to work independently and fulfill my duties with minimal supervision.

During the Summer of 1995 I assisted Professor Rivest with the design of the new course "Computer and Network Security". The job included the preparation on the new curriculum, choice of the topics to be covered and research on such topics.

Teaching is a fundamental aspect of my professional goals and I look forward to taking teaching responsibilities. Since a university remains competitive and successful only if it teaches state-of-the-art course, I intend to be actively involved in the development of undergraduate and graduate curricula. My experience with Professor Rivest on the design from scratch of a new course has taught me much about the skills needed in order to incorporate new material in existing courses and/or teach new ones.

Thanks to the broad training received during my graduate career at MIT, I believe I can teach almost any undergraduate course in computer science. However the courses I feel best qualified to teach are "Cryptography", "Computer and Network Security" and "Algorithms", due to my research interests and my previous teaching experience at MIT. I am also interested in teaching other courses such as distributed algorithms, operating systems, theory of computation, complexity theory, machine learning, artificial intelligence, logic.