ROSARIO GENNARO

Curriculum Vitae (7/2016)

Center for Algorithms and Interactive Scientific Software, City College of the City University of New York, Shephard Hall 279, 160 Convent Avenue New York, NY 10031. Email: rosario@cs.ccny.cuny.edu

Professional Interests

My scientific research is mainly concentrated in the area of Cryptography. The main focus of my research is theoretical and mathematical, but always motivated by real-life practical applications.

Education

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

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

Università di Catania.
Laurea in Matematica, *summa cum laude*, November 1989.
Thesis Title: *Algoritmi di Geometria Computazionale e loro Applicazioni.*
Supervisor: Prof. Alfredo Ferro.

Work Experience

City College.
2012-current: Full Professor in the Computer Science Department. Also Director of the Center for Algorithms and Interactive Scientific Software, leading the Center's staff in theoretical and applied research in cryptography.

IBM Research.
1996-2012: Research Staff Member in the Cryptography Research group at the T.J.Watson Research Center, doing theoretical and mathematical research in cryptography.

MIT Laboratory for Computer Science.
1990-1996: Research Assistant in the Theory of Computation group. Research areas: Cryptography, distributed computation, learning theory, computational algebra. Supervisor: Prof. Silvio Micali.

Massachusetts Dept. of Public Health
Summer 1996: Consultant. Worked in conjunction with an epidemiologist on a project studying cases of domestic violence. Implemented an encryption program to work with the statistical package used to collect data for the study.

Dipartimento di Matematica, Università di Catania.
6/1989–6/1990: Research Assistant. Worked on a team implementing an automated theorem prover for theorems in elementary geometry. Supervisor: Prof. Alfredo Ferro.

Teaching

City College of New York.
2012-now: Professor. Classes taught include CSc486 "Introduction to Complexity Theory"; CSc220 "Algorithms" and doctoral seminars at the CUNY Graduate Center.

Columbia University Department of Computer Science.
Fall 2010: Adjunct Professor teaching a graduate-level course on Introduction to Cryptography.

Dipartimento di Matematica e Informatica, Università di Catania.
Academic Year 2009-10: Visiting Professor teaching various graduate-level courses on topics of Cryptography.

Polytechnic University of Catalunya, Department of Applied Mathematics.
Summer 2004: Visiting Professor teaching a graduate-level course on Provable Security and Efficiency in Cryptographic Constructions.

Columbia University Department of Electrical Engineering.
Spring 1998: Adjunct Professor teaching a graduate-level course on Cryptography and Network Security.

MIT Department of Electrical Engineering and Computer Science
1992-1995: Teaching Assistant for the following courses:

- 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. Supervisor: Prof. Ronald Rivest.
- Theory of Algorithms, (4 semesters in both the undergraduate and graduate versions.) Supervisors: Proff. Silvio Micali, Shafi Goldwasser, Bonnie Berger.

Awards

Outstanding Innovation Award granted by IBM Research in 2011 for Contributions to Threshold and Proactive Security.

Keynote Speaker at the 2013 ESORICS Trustworthy Clouds Workshop (London, UK, September 2013)

KEYNOTE SPEAKER at the 2013 International Conference on Cryptology and Network Security (CANS) (Paraty, Brazil, November 2013)

Grants

PRINCIPAL INVESTIGATOR NSF Large Grant on *Verifiable Hardware: Chips that Prove their Own Correctness*, $3M among 6 PI's, 2016-2021.

PRINCIPAL INVESTIGATOR NSF EAGER Grant on *Economic Incentives for Correct Outsourced Computation via Rational Proofs*, $75K, 2015–2017.

PRINCIPAL INVESTIGATOR Department of Homeland Security grant on *Highly Efficient Protocols for Secure Search Over Encrypted Documents*, $50K, 2015-2016

PRINCIPAL INVESTIGATOR International Technological Alliance (US Army/UK Department of Defence) grant, $450K (CUNY portion), 2011-2016.

PRINCIPAL INVESTIGATOR NSF Grant on *Cryptographic Algorithms for Security in Cloud Computing Applications*, $500K, 2010–2014.

Professional Activities

PROGRAM CO-CHAIR for the 2014 and 2015 CRYPTO Conference.

PROGRAM CHAIR for the 2008 Applied Cryptography and Network Security (ACNS'08) and the 2011 Public Key Cryptography (PKC'11) Conferences.

GENERAL CHAIR for the 2012 Theory of Cryptography Conference (TCC'12).

PROGRAM COMMITTEE MEMBER for the following conferences: CRYPTO (1999 and 2007), EUROCRYPT (2002, 2004, 2010 and 2013), ASIACRYPT (2001 and 2013); Theory of Cryptography Conference (TCC 2005 and 2013); Workshop on Public Key Cryptography (PKC 2006, 2008, 2009, 2012 and 2013); Crypto Track of the RSA Security Conference (CT-RSA 2001, 2003, 2004 and 2006); 2006 IEEE Conference on Trustworthy Network Computing; 2008 and 2009 USENIX Workshop on Emerging Voting Technology; 2008 Conference on Security in Communication Networks; IFIFP TCS2000, the International Conference on Theoretical Computer Informatics.

REVIEWER for the following academic journals: Journal of the ACM, SIAM Journal on Computing, IEEE Transactions on Information Theory, IEEE Transactions on Computers, Journal of Computers and System Sciences, Information and Computation, Journal of Cryptology, Theoretical Computer Science.

Reviewer for the following annual conferences: CRYPTO, EUROCRYPT, ACM Symposium of Theory of Computing (STOC), IEEE Foundations of Computer Science (FOCS), International Colloquium on Automata Languages and Programming (ICALP), ACM Symposium on Principles of Distributed Computing (PODC).

MEMBER of the International Association of Cryptologic Research (IACR)

Students Supervised

Current doctoral students: Matteo Campanelli, Konstantinos Vamvourellis, Nihal Vatandas.

Past Students: Dario Catalano and Mario Di Raimondo (doctoral students in Computer Science at the University of Catania, Italy – supervised while at IBM Research).

Publications

International Journals

1. D. Catalano, D. Fiore and R. Gennaro. *A Certificateless Approach to Onion Routing.* To appear in the International Journal of Information Security. Preliminary version in [52].

2. R. Gennaro, C. Hazay and J. Sorensen. *Automata Evaluation and Text Search Protocols with Simulation Based Security.* J. Cryptology 29(2): 243-282 (2016). Preliminary version in [50].

3. D. Catalano, D. Fiore, R. Gennaro and K. Vamvourellis. *Algebraic (trapdoor) one-way functions: Constructions and applications.* Theor. Comput. Sci. 592: 143-165 (2015) Preliminary version in [40].

4. E. Bresson, D. Catalano, M. Di Raimondo, D. Fiore and R. Gennaro. *Off-line/online signatures revisited: a general unifying paradigm, efficient threshold variants and experimental results.* Int. J. Inf. Sec. 12(6): 439-465 (2013)

5. D. Catalano, M. Di Raimondo, D. Fiore, R. Gennaro, O. Puglisi. *Fully non-interactive onion routing with forward secrecy.* Int. J. Inf. Sec. 12(1): 33-47 (2013)

6. D. Fiore, R. Gennaro and N.P. Smart. *Relations between the security models for Certificateless Encryption and ID-Based Key Agreement.* Int. J. Inf. Sec. 11(1): 1–22 (2012). Preliminary version in [46].

7. D. Fiore and R. Gennaro. *Identity-Based Key Exchange protocols without Pairings,* Springer Transactions on Computational Sciences vol.X Special Issue on Security on Computing, Part 1, pp.42–77, December 2010. Preliminary version in [51].

8. Y. Desmedt, R. Gennaro, K. Kurosawa and V. Shoup. *A New and Improved Paradigm for Hybrid Encryption secure against Chosen-Ciphertext Attack.* J. of Cryptology 23(1):91–120 (2010).

9. M. Di Raimondo and R. Gennaro. *New Approaches for Deniable Authentication.* J.l of Cryptology 22(4): 572-615 (2009). Preliminary version in [61].

10. M. Abe, R. Gennaro and K. Kurosawa. *Tag-KEM/DEM: A New Framework for Hybrid Encryption.* J. Cryptology 21(1):97-130 (2008). Preliminary version in [63].

11. R. Gennaro, S. Jarecki, H. Krawczyk and T. Rabin. *Secure Distributed Key Generation for Discrete-Log Based Cryptosystems.* J. Cryptology 20(1):51-83 (2007). Preliminary version in [70, 87].

12. D. Catalano and R. Gennaro. *Cramer-Damgard Signatures Revisited: Efficient Flat-Tree Signatures Based on Factoring.* Theor. Comput. Sci. 370(1-3):186-200 (2007). Preliminary version in [64].

13. R. Gennaro and Y. Lindell. *A Framework for Password-Based Authenticated Key Exchange.* ACM Trans. Inf. Syst. Secur. 9(2):181-234 (2006). Preliminary version in [72].

14. M. Di Raimondo and R. Gennaro. *Provably Secure Threshold Password-Authenticated Key Exchange.* J. of Computer and System Sciences, 72:978–1001, Elsevier (2006). Preliminary version in [71].

15. R. Gennaro, Y. Gertner, J. Katz and L. Trevisan. *Bounds on the efficiency of generic Cryptographic Constructions.* SIAM J. on Computing, 35(1): 217-246 (2005). Preliminary versions in [80,73].

16. M. Di Raimondo and R. Gennaro. *Secure Multiplication of Shared Secrets In The Exponent.* Information Processing Letters, 96(2):71–79, Elsevier, October 2005.

17. R. Gennaro. *An Improved Pseudo-random Generator Based on the Discrete Logarithm Problem.* Journal of Cryptology, 18(2):91–110, Spring 2005. Springer. A preliminary version appears in [81].

18. D. Catalano, R. Gennaro, N. Howgrave-Graham. *Paillier's Trapdoor Function Hides up to $O(n)$ bits.* Journal of Cryptology, 15(4):251–269, Fall 2002. Springer. A preliminary version appears in [79].

19. V. Shoup and R. Gennaro. *Securing Threshold Cryptosystems against Chosen Ciphertext Attack.* Journal of Cryptology, 15(2):75–96, Spring 2002. Springer. A preliminary version appears in [92].

20. R. Gennaro and P. Rohatgi. *How to Sign Digital Streams.* Information and Computation 165, pp.100–116, 2001. A preliminary version appears in [94].

21. R. Gennaro, S. Jarecki, H. Krawczyk and T. Rabin. *Robust Threshold DSS Signatures.* Information and Computation 164, pp.54–84, 2001. A preliminary version appears in [99].

22. J. Garay, R. Gennaro, C. Jutla and T. Rabin. *Secure Distributed Storage and Retrieval.* Theoretical Computer Science 243(1-2):363–389 (2000). A preliminary version appears in [93].

23. D. Catalano and R. Gennaro. *New Efficient and Secure Protocols for Verifiable Signature Sharing and Other Applications.* Journal of Computer and System Sciences, 61(1):51–80, August 2000. A preliminary version appears in [89].

24. R. Gennaro, H. Krawczyk and T. Rabin. *RSA-Based Undeniable Signatures.* Journal of Cryptology, 13(4):397–416, June 2000. A preliminary version appears in [95].

25. R. Gennaro *A Protocol to Achieve Independence in Constant Rounds.* IEEE Transactions on Parallel and Distributed Systems, 11(3):636–647, July 2000. A preliminary version appears in [101].

26. R. Gennaro, S. Jarecki, H. Krawczyk and T. Rabin. *Robust and Efficient Sharing of RSA Functions.* J. of Cryptology, 13(2):273–300, March 2000. A preliminary version appears in [98].

27. R. Gennaro, H. Krawczyk and T. Rabin. *Undeniable Certificates.* Electronic Letters, 35(20):1723–1724, September 1999.

28. R. Cramer, R. Gennaro and B. Schoenmakers. *A Secure and Optimally Efficient Multi-Authority Election Scheme.* European Transactions of Telecommunications 8(5), September 1997. A preliminary version appears in [96].

29. R. Gennaro, P. Karger, S. Matyas, M. Peyravian, A. Roginsky, D. Safford, M. Willett, N. Zunic. *Secure Key Recovery.* Computers and Security Vol.16, 1997. Also IBM Technical Report 29.2273

Refereed Conferences

30. R. Gennaro, S. Goldfeder and A. Narayanan. *Threshold-Optimal DSA/ECDSA Signatures and an Application to Bitcoin Wallet Security.* ACNS 2016, Springer-Verlag Lecture Notes in Computer Science, No.9696, pp.156-174.

31. M. Campanelli and R. Gennaro. *Sequentially Composable Rational Proofs.* GameSec 2015, Springer-Verlag Lecture Notes in Computer Science, No.9406 , pp. 270-288.

32. W. Drazen, E. Ekwedike and R. Gennaro. *Highly Scalable Verifiable Encrypted Search.* IEEE Workshop on Security and Privacy in the Cloud. 2015, IEEE Press.

33. D. Fiore, R. Gennaro and V. Pastro. *Efficiently Verifiable Computation on Encrypted Data.* 2014 ACM Conference on Computer and Communication Security, pp.844–855.

34. J. Soryal, I. M. Perera, I. Darwish, N. Fazio, R. Gennaro, T.N. Saadawi. *Combating Insider Attacks in IEEE 802.11 Wireless Networks with Broadcast Encryption.* 28th IEEE International Conference on Advanced Information Networking and Applications, AINA 2014, pp.472-479, IEEE 2014

35. D. Catalano, D. Fiore, R. Gennaro and L. Nizzardo. *Generalizing Homomorphic MACs for Arithmetic Circuits.* 2014 Conference on Public Key Cryptography (PKC'14), Springer-Verlag Lecture Notes in Computer Science, No.8383 , pp. 538-555.

36. J. Alwen, M. Barbosa, P. Farshim, R. Gennaro, S. Gordon, S. Tessaro and D.A. Wilson. *On the Relationship between Functional Encryption, Obfuscation, and Fully Homomorphic Encryption.* IMA Int. Conf. 2013, Springer-Verlag Lecture Notes in Computer Science, No.8308, pp. 65-84

37. R. Gennaro and D. Wichs. *Fully Homomorphic Message Authenticators.* ASIACRYPT 2013. Springer-Verlag Lecture Notes in Computer Science, No.8270, pp. 301–320.

38. N. Fazio, R. Gennaro, I. M. Perera, W. E. Skeith III. *Hardcore Predicates for a Diffie-Hellman Problem over Finite Fields.* CRYPTO 2013, Springer-Verlag Lecture Notes in Computer Science, No.8043, pp. 148–165.

39. R. Gennaro, C. Gentry, B. Parno and M. Raykova. *Quadratic Span Programs and Succint Non-Interactive Zero-Knowledge Proofs.* EUROCRYPT 2013. Springer-Verlag Lecture Notes in Computer Science, No.7881, pp. 626–645.

40. D.Catalano, D.Fiore, R.Gennaro and K.Vamvourellis. *Algebraic (Trapdoor) One Way Functions and their Applications.* 2013 Theory of Cryptography Conference (TCC), Springer-Verlag Lecture Notes in Computer Science, No.7785, pp. 680-699.

41. S. Ames, R. Gennaro, M. Venkitasubramaniam. *The Generalized Randomized Iterate and Its Application to New Efficient Constructions of UOWHFs from Regular One-Way Functions.* ASIACRYPT 2012 Springer-Verlag Lecture Notes in Computer Science, No.7658, pp. 154-171.

42. D. Fiore, R. Gennaro. *Publicly verifiable delegation of large polynomials and matrix computations with applications.* 2012 ACM Conference on Computer and Communications Security (CCS), pp. 501-512.

43. D. Dachman-Soled, R. Gennaro, H. Krawczyk and T. Malkin. *Computational Extractors and Pseudorandomness.* 2012 Theory of Cryptography Conference (TCC) Springer Lecture Notes in Computer Science No. 7194, pp. 383-403.

44. S. Benabbas, R. Gennaro and Y. Vahlis. *Verifiable Delegation of Computation over Large Datasets.* CRYPTO 2011, Lecture Notes in Computer Science no.6841, pp.111–131, Springer 2011.

45. D. Catalano, M. Di Raimondo, D. Fiore, R. Gennaro and O. Puglisi. *Fully Non-interactive Onion Routing with Forward-Secrecy.* Proceedings of the 2011 Conference on Applied Cryptography and Network Security (ACNS'11), Lecture Notes in Computer Science no.6715, pp.255–273, Springer 2011.

46. D. Fiore, R. Gennaro and N.P. Smart. *Constructing Certificateless Encryption and ID-Based Encryption from ID-Based Key Agreement.* Proceedings of the Fourth International Conference on Pairing-Based Cryptography (PAIRING'10), Lecture Notes in Computer Science no.6487, pp.167–186.

47. R. Gennaro, C. Gentry and B. Parno. *Non-interactive Verifiable Computing: Outsourcing Computation to Untrusted Workers.* Proceedings of CRYPTO 2010, Lecture Notes in Computer Science no.6223, pp.465-482, Springer 2010.

48. R. Gennaro, H. Krawczyk and T. Rabin. *Okamoto-Tanaka Revisited: Fully Authenticated Diffie-Hellman with Minimal Overhead.* Proceedings of the 2010 Conference on Applied Cryptography and Network Security (ACNS'10), Lecture Notes in Computer Science no.6123, pp.309-328, Springer 2010.

49. R. Gennaro, J. Katz, H. Krawczyk and T. Rabin. *Secure Network Coding over the Integers.* Proceedings of the 2010 Public Key Cryptography Conference (PKC'10), Lecture Notes in Computer Science no.6056, pp.142–160, Springer 2010.

50. R. Gennaro, C. Hazay and J. Sorensen. *Text Search Protocols with Simulation Based Security.* Proceedings of the 2010 Public Key Cryptography Conference (PKC'10), Lecture Notes in Computer Science no.6056, pp.332-350, Springer 2010.

51. D. Fiore and R. Gennaro. *Making the Diffie-Hellman Protocol Identity-Based.* Proceedings of the 2010 Crypto Track of the RSA Security Conference (CT-RSA'10), Lecture Notes in Computer Science no.5985, pp.165-178, Springer 2010.

52. D. Catalano, D. Fiore and R. Gennaro. *Certificateless onion routing.* Proceedings of the 2009 ACM Conference on Computer and Communications Security (CCS'09), pp.151-160, ACM Press 2009.

53. R. Gennaro and S. Halevi. *More on Key Wrapping.* Proceedings of the 2009 Workshop on Selected Areas in Cryptography (SAC'09), Lecture Notes in Computer Science no.5867, pp.53–70, Springer 2009.

54. R. Gennaro, S. Halevi, H. Krawczyk, T. Rabin, S. Reidt and S. D. Wolthusen. *Strongly-Resilient and Non-interactive Hierarchical Key-Agreement in MANETs.* Proceedings of the 2008 European Symposium on Research in Computer Security (ESORICS'08), Lecture Notes in Computer Science no.5283, pp.49-65, Springer, 2008.

55. R. Gennaro, S. Halevi, H. Krawczyk and T. Rabin. *Threshold RSA for Dynamic and Ad-Hoc Groups.* Proceedings of EUROCRYPT 2008, Lecture Notes in Computer Science no.4965, pp.88-107, Springer, 2008.

56. D. Catalano, M. Di Raimondo, D. Fiore and R. Gennaro. *Off-Line/On-Line Signatures: Theoretical Aspects and Experimental Results.* Proceedings of Public Key Cryptography 2008 (PKC'08), Lecture Notes in Computer Science no.4939, pp.101-120, Springer, 2008.

57. R. Gennaro. *Faster and Shorter Password-Authenticated Key Exchange.* Proceedings of the 2008 Theory of Cryptography Conference (TCC'08), Lecture Notes in Computer Science no.4948, pp.589-606, Springer, 2008.

58. E. Bresson, D. Catalano and R. Gennaro. *Improved On-Line/Off-Line Threshold Signatures.* Proceedings of Public Key Cryptography 2007 (PKC'07), Lecture Notes in Computer Science no.4450, pp.217-232, Springer, 2008.

59. M. Di Raimondo, R. Gennaro and H. Krawczyk. *Deniable Authentication and Key Exchange.* Proceedings of the 2006 ACM Conference on Computer and Communication Security, (CCS'06), pp.400-409, Alexandria VA, November 2005.

60. R. Gennaro and S. Micali. *Independent Zero-Knowledge Sets.* Proceedings of ICALP 2006, Lecture Notes in Computer Science no.4052, pp.34-45, Springer 2006.

61. M. Di Raimondo and R. Gennaro. *New Approaches for Deniable Authentication.* Proceedings of the 2005 ACM Conference on Computer and Communication Security, (CCS'05), Alexandria VA, November 2005. Final version in [9].

62. M. Di Raimondo, R. Gennaro and H. Kawczyk. *The Security of "Off-the-Record Messaging".* Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, (WPES'05), Alexandria VA, November 2005.

63. M Abe, R. Gennaro, K. Kurosawa and V. Shoup. *Tag-KEM/DEM: A New Framework for Hybrid Encryption and A New Analysis of Kurosawa-Desmedt KEM.* Proceedings of EUROCRYPT'05, Lecture Notes in Computer Science no.3494, pp.128-146, Springer 2005.

64. D. Catalano and R. Gennaro. *Cramer-Damgard Signatures Revisited: Efficient Flat-Tree Signatures Based on Factoring.* Proceedings of Public Key Cryptography 2005 (PKC'05), Lecture Notes in Computer Science no.3386, pp.313-327, Springer 2005. Final version in [12].

65. R. Gennaro, D. Leigh, R. Sundaram and W.S. Yerazunis. *Batching Schnorr Identification Scheme with Applications to Privacy-Preserving Authorization and Low-Bandwidth Communication Devices.* Proceedings of ASIACRYPT'04, Lecture Notes in Computer Science no.3329, pp.276–292, Springer 2004.

66. R. Gennaro. *Multi-trapdoor Commitments and Their Applications to Proofs of Knowledge Secure Under Concurrent Man-in-the-Middle Attacks.* Proceedings of CRYPTO'04, Lecture Notes in Computer Science no.3152, pp.220–236, Springer 2004.

67. Y. Dodis, R. Gennaro, J. Hastad, H. Krawczyk and T. Rabin. *Randomness Extraction and Key Derivation Using the CBC, Cascade and HMAC Modes.* Proceedings of CRYPTO'04, Lecture Notes in Computer Science no.3152, pp.494–510, Springer 2004.

68. R. Gennaro, H. Krawczyk and T. Rabin. *Secure Hashed Diffie-Hellman over Non-DDH Groups.* Proceedings of EUROCRYPT'04, Lecture Notes in Computer Science no.3027, pp.361–381, Springer 2004.

69. R. Gennaro, A. Lysyanskaya, T. Malkin, S. Micali and T. Rabin. *Algorithmic Tamper-Proof (ATP) Security: Theoretical Foundations for Security against Hardware Tampering.* Proceedings of the 2004 Theory of Cryptography Conference (TCC'04), Lecture Notes in Computer Science no.2951, pp.258-277, Springer 2004.

70. R. Gennaro, S. Jarecki, H. Krawczyk and T. Rabin. *Secure Applications of Pedersen's Distributed Key Generation Protocol.* Proceedings of Crypto Track of the 2003 RSA Security Conference (CT-RSA'03), Lecture Notes in Computer Science no.2612, pp.373–390, Springer 2003. The final version appears in [11].

71. M. Di Raimondo and R. Gennaro. *Provably Secure Threshold Password-Authenticated Key Exchange.* Proceedings of EUROCRYPT'03, Lecture Notes in Computer Science no.2656, pp.507–523, Springer 2003. Final version in [14].

72. R. Gennaro and Y. Lindell. *A Framework for Password-Based Authenticated Key Exchange.* Proceedings of EUROCRYPT'03, Lecture Notes in Computer Science no.2656, pp.524-543, Springer 2003. The final version appears in [13].

73. R. Gennaro, Y. Gertner and J. Katz. *Lower bounds on the efficiency of encryption and digital signature schemes.* Proceedings of the 2003 ACM Symposium on the Theory of Computing (STOC'03), pp.417-425. ACM Press. The final version appears in [15].

74. R. Gennaro, Y. Ishai, E. Kushilevitz and T. Rabin. *On 2-Round Secure Multiparty Computations.* Proceedings of CRYPTO'02. Lecture Notes in Computer Science no.2442, pp.178-193. Springer 2002.

75. R. Gennaro and D. Micciancio. *Cryptanalysis of a Pseudorandom Generator Based on Braid Groups* Proceedings of EUROCRYPT'02. Lecture Notes in Computer Science no.2332, pp.1–13. Springer 2002.

76. D. Catalano, R. Gennaro, N. Howgrave-Graham and P. Nguyen. *Paillier's Cryptosystem Revisited.* To appear in the Proceedings of the 2001 Conference on Computer and Communications Security (CCS'01). ACM Press.

77. R. Gennaro, Y. Ishai, E. Kushilevitz and T. Rabin. *The Round Complexity of Verifiable Secret Sharing and Secure Multicast.* Proceedings of the 2001 ACM Symposium on the Theory of Computing (STOC'01), pp.580–589. ACM Press.

78. N. Howgrave-Graham, J. Dyer and R. Gennaro. *Pseudo-Random Number Generation on the IBM 4758 Secure Crypto Coprocessor.* Proceedings of the 2001 Workshop on Cryptographic Hardware and Embedded Systems (CHES'01). Lecture Notes in Computer Science, vol.2162, pp.93–102, Springer.

79. D. Catalano, R. Gennaro, N. Howgrave-Graham. *The Bit Security of Paillier's Encryption Scheme and its Applications.* Proceedings of EUROCRYPT'2001, Lecture Notes in Computer Science, vol.2045, pp.229–243, Springer. The final version appears in [18].

80. R. Gennaro and L. Trevisan. *Lower Bounds on the Efficiency of Generic Cryptographic Constructions.* Proceedings of the 2000 IEEE Symposium on the Foundations of Computer Science (FOCS'2000), pp.305–313, IEEE Press. The final version appears in [15].

81. R. Gennaro, *An Improved Pseudo-Random Generator Based on Discrete Log.* Proceedings of CRYPTO'2000, Lecture Notes in Computer Science, vol.1880, pp.469–481, Springer-Verlag. The final version appears in [17].

82. D. Catalano, R. Gennaro and S. Halevi. *Computing inverses over a shared secret modulus.* Proceedings of EUROCRYPT'2000, Lecture Notes in Computer Science, vol.1807, pp.190–206, Springer-Verlag.

83. S. Battiato, D. Catalano, G. Gallo and R. Gennaro. *A color opponency watermarking scheme for digital images.* 2000 IST/SPIE International Symposium on Electronic

Imaging. Proceedings of the International Society for Optical Engineering (SPIE), vol.3971, pp. 510-515, 2000.

84. S. Battiato, D. Catalano, G. Gallo and R. Gennaro. *Robust Watermarking for Images Based on Color Manipulation.* Proceedings of the 1999 Workshop on Information Hiding, Lecture Notes in Computer Science vol.1768, pp.301–315, Springer-Verlag.

85. R. Canetti, R. Gennaro, S. Jarecki, H. Krawczyk and T. Rabin. *Adaptive Security for Threshold Cryptosystems.* Proceedings of CRYPTO'99, Lecture Notes in Computer Science, vol.1666, pp.98–115, Springer–Verlag.

86. R. Gennaro, S. Halevi and T. Rabin. *Secure Hash-and-Sign Signatures Without the Random Oracle.* Proceedings of EUROCRYPT'99, Lecture Notes in Computer Science, vol.1592, pp.123–139, Springer–Verlag.

87. R. Gennaro, S. Jarecki, H. Krawczyk and T. Rabin. *Secure Distributed Key Generation for Discrete-Log Based Cryptosystems.* Proceedings of EUROCRYPT'99, Lecture Notes in Computer Science, vol.1592, pp.295–310, Springer–Verlag. The final version appears in [11].

88. R. Gennaro, D. Micciancio and T. Rabin. *An Efficient Non-Interactive Statistical Zero-Knowledge Proof System for Quasi-Safe Prime Products.* Proceedings of the 1998 ACM Conference on Computer and Communications Security (CCS'98), pp.67–72, ACM Press.

89. D. Catalano and R. Gennaro. *New Efficient and Secure Protocols for Verifiable Signature Sharing and Other Applications.* Proceedings of CRYPTO'98, Lecture Notes in Computer Science, vol.1462, pp.105–120, Springer–Verlag. The final version appears in [23].

90. C. Burwick, D. Coppersmith, E. D'Avignon, R. Gennaro, S. Halevi, C. Jutla, S.M. Matyas Jr., L. O'Connor, M. Peyravian, D. Safford, and N. Zunic. *MARS – A candidate cipher for AES.* Proceedings of the First Advanced Encryption Standard Candidate Conference, NIST, 1998.

91. R. Gennaro, M. Rabin and T. Rabin. *Simplified VSS and Fast-Track Multiparty Computation with Applications to Threshold Cryptography.* Proceedings of the 1998 ACM Symposium on Principles of Distributed Computation, (PODC 1998), pp. 101–111, ACM Press.

92. V. Shoup and R. Gennaro. *Securing Threshold Cryptosystems against Chosen Ciphertext Attack.* Proceedings of EUROCRYPT'98, Lecture Notes in Computer Science, vol.1403, pp.1–16, Springer–Verlag.

93. J. Garay, R. Gennaro, C. Jutla and T. Rabin. *Secure Distributed Storage and Retrieval.* Proceedings of the 1997 Workshop on Distributed Algorithms (WDAG'97), Lecture Notes in Computer Science vol.1320, pp.275–289, Springer–Verlag. The final version appears in [22].

94. R. Gennaro and P. Rohatgi. *How to Sign Digital Streams.* Proceedings of CRYPTO'97, Lecture Notes in Computer Science vol.1294, pp.180–197, Springer–Verlag. The final version appears in [20].

95. R. Gennaro, H. Krawczyk and T. Rabin. *RSA-Based Undeniable Signatures.* Proceedings of CRYPTO'97, Lecture Notes in Computer Science vol.1294, pp.132–149, Springer–Verlag. The final version appears in [24].

96. R. Cramer, R. Gennaro and B. Schoenmakers. *A Secure and Optimally Efficient Multi-Authority Election Scheme.* Proceedings of EUROCRYPT'97, Lecture Notes in Computer Science vol. 1233, pp. 103–118, Springer–Verlag. The final version appears in [28].

97. R. Canetti and R. Gennaro. *Incoercible Multiparty Computation.* Proceedings of the 1996 IEEE Symposium on the Foundations of Computer Science (FOCS'96), pp.504–513, IEEE Press.

98. R. Gennaro, S. Jarecki, H. Krawczyk and T. Rabin. *Robust and Efficient Sharing of RSA Functions.* Proceedings of CRYPTO'96, Lecture Notes in Computer Science vol.1109, pp.157-172, Springer–Verlag. The final version appears in [26].

99. R. Gennaro, S. Jarecki, H. Krawczyk and T. Rabin. *Robust Threshold DSS Signatures.* Proceedings of EUROCRYPT'96, Lecture Notes in Computer Science vol.1070, pp.354–371, Springer–Verlag. The final version appears in [21].

100. R. Gennaro and S. Micali. *Verifiable Secret Sharing as Secure Computation.* Proceedings of EUROCRYPT'95, Lecture Notes in Computer Science vol.921, pp.168-182, Springer–Verlag.

101. R. Gennaro, *Achieving Independence Efficiently and Securely.* Proceedings of the 1995 ACM Symposium on Principles of Distributed Computation, (PODC 1995), pp.130–136, ACM Press. The final version appears in [25].

102. S. Decatur and R. Gennaro. *On Learning from Noisy or Incomplete Examples.* Proceedings of the 1995 ACM Conference on Computational Learning Theory, (COLT'95), pp.353–360, ACM Press.

103. 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. Lecture Notes in Artificial Intelligence vol.1360, pp.87-101, Springer–Verlag, 1997.

Books and Book Chapters

104. R. Gennaro and M. Robshaw. *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings*, Lecture Notes in Computer Science 9215-9216, Springer.

105. J.A. Garay and R. Gennaro . *Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings.* Lecture Notes in Computer Science 8616-8617, Springer.

106. D. Catalano, N. Fazio, R. Gennaro, A. Nicolosi, (Eds.): *Public Key Cryptography - PKC 2011: 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6-9, 2011. Proceedings.* Lecture Notes in Computer Science 6571, Springer 2011,

107. S.M. Bellovin, R. Gennaro, A.D. Keromytis, M. Yung (Eds.): *Applied Cryptography and Network Security, 6th International Conference, ACNS 2008, New York, NY, USA, June 3-6, 2008. Proceedings.* Lecture Notes in Computer Science 5037, Springer 2008,

108. R. Gennaro. *Cryptographic Algorithms for Multimedia Traffic.* In *Foundations of Security Analysis and Design II*, R. Focardi and R. Gorrieri eds. Lecture Notes in Computer Science no.2946, Springer 2004

Newsletters and Magazines

109. R. Gennaro. *Randomness in Cryptography.* IEEE Security & Privacy 4(2): 64-67 (2006)

110. R. Canetti, R. Gennaro, A. Herzberg, D. Naor, *Proactive Security: Long-term Protection Against Break-ins.* RSA Laboratories' *CryptoBytes*, vol.3, no.1, Spring 1997.

Technical Reports

111. R. Gennaro, S. Matyas, M. Peyravian, A. Roginsky, M. Willett, N. Zunic. *Fault-Based Attacks on Cryptosystems.* IBM Technical Report 29.2225

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

113. R. Gennaro and A. Shamir, *Partial Cryptanalysis of Koyama's encryption scheme.* MIT Laboratory for Computer Science Technical Memo no.512.

Patents

1. R. Gennaro and C. Tresser. *Electronic Cash Controlled by Non-Homomorphic Signatures.* US Patent no.7640432

2. R. Gennaro, S. Halevi, T. Rabin. *Secure hash-and-sign signatures.* US Patent no.6578144

3. C.S. Chandersekaran, R. Gennaro, S. Gupta, S.M. Matyas, D. Safford, N. Zunic. *Method and apparatus for providing interoperability between key recovery and non-key recovery systems.* US Patent no.6535607

4. R. Gennaro, S. Halevi, S. Maes, T. Rabin, J. Sorensen. *Biometric authentication system with encrypted models.* US Patent no.6317834

5. R. Gennaro, H. Krawczyk, T. Rabin. *Undeniable certificates for digital signature verification.* US Patent no.6292897

6. D. Coppersmith, R. Gennaro, S. Halevi, C.S. Jutla, S.M. Matyas, M. Peyravian, D. Safford, N. Zunic. *Method and apparatus for advanced symmetric key block cipher with variable length key and block.* US Patent no.6243470

7. D. Coppersmith, R. Gennaro, S. Halevi, C.S. Jutla, S.M. Matyas, M. Peyravian, D. Safford, N. Zunic. *Method and apparatus for advanced byte-oriented symmetric key block cipher with variable.* US Patent no.6192129.

8. D. Coppersmith, R. Gennaro, S. Halevi, C.S. Jutla, S.M. Matyas, L. O'Connor, M. Peyravian, D. Safford, N. Zunic. *Symmetric block cipher using multiple stages with modified type-1 and type-3 feistel networks.* US Patent no.6189095.

9. D. Coppersmith, R. Gennaro, S. Halevi, C.S. Jutla, S.M. Matyas, L. O'Connor, M. Peyravian, D. Safford, N. Zunic. *Method and apparatus for a symmetric block cipher using multiple stages with type-1 and type-3 feistel networks.* US Patent no.6185679.

10. D. Coppersmith, R. Gennaro, S. Halevi, C.S. Jutla, S.M. Matyas, L. O'Connor, M. Peyravian, D. Safford, N. Zunic. *Method and apparatus for a symmetric block cipher using multiple stages.* US Patent no.6185304.

11. C.S. Chandersekaran, R. Gennaro, S. Gupta, S.M. Matyas, D. Safford, N. Zunic. *Method and apparatus for interoperable validation of key recovery information in a cryptographic system.* US Patent no. 6058188.

12. R. Gennaro, P. Rohatgi. *How to Sign Digital Streams.* US Patent no.6009176 and no.6311271.

13. J. Garay, R. Gennaro, C. Jutla, T. Rabin. *Method and apparatus for the secure distributed storage and retrieval of information.* US Patents no.5991414 and no.6192472

14. R. Gennaro, D. Johnson, P. Karger, S. Matyas, M. Peyravian, D. Safford, M. Yung, N. Zunic. *Two-phase cryptographic key recovery system.* US Patent no.5937066.

15. R. Gennaro, P. Karger, S. Matyas, M. Peyravian, D. Safford, N. Zunic. *Method and apparatus for verifiably providing key recovery information in a cryptographic system.* US Patent no.5907618.

Invited Seminars

1. *Sequentially Composable Rational Proofs.* 2015 New York Colloquium on Algorithms and Complexity - 2015 Summer Program on Cryptography at the Simons Institute for Theoretical Computer Science, Berkeley.

2. *Verifiable Computation.* Three-lecture course at the International Summer School on Information Security, Bilbao, Spain, July 2015.

3. *A Survey of Verifiable Computation.* Keynote talk at the at the 2013 ESORICS Trustworthy Clouds Workshop (London, UK, September 2013) and the 2013 International Conference on Cryptology and Network Security (CANS) (Paraty, Brazil, November 2013)

4. *Hardcore Predicates for a Diffie-Hellman Problem over Finite Fields.* AMS Spring Sectional Meeting, Boston, April 2013; Geometric and Asymptotic Group Theory Conference, City College, May 2013.

5. *Non-Interactive Verifiable Computing: Outsourcing Computation to Untrusted Workers.* MITACS Seminar Series on Privacy, University of Waterloo, March 2010; NYU Polytechnic, March 2011; U. of Pennsylvania Theory Seminar October 2011; Stanford University Security Seminar, November 2011; NY Area Security and Privacy Research Day, December 2011.

6. *Text Search Protocols with Simulation Based Security.* Workshop on Security in Cloud Computing. MIT CSAIL, Cambridge MA, August 2010.

7. *Provable Security and Efficiency in Cryptographic Constructions.* Three-lecture course at the Fourteenth Estonian Winter School in Computer Science (University of Tartu, Estonia). March 2009.

8. *Identity-Based Key Exchange Protocols.* Carnegie-Mellon University, CyLab Seminar Series, January 2009.

9. *Provable Security vs. Efficiency in Cryptographic Algorithms.* John Hopkins University, Computer Science Dept, Distinguished Lecture Series. October 2007.

10. *Faster and Shorter Password-Authenticated Key Exchange.* NYU Cryptography Seminar. Spring 2007.

11. *Deniable Authentication and Key Exchange.* IBM Research Security Seminar, November 2006.

12. *Tag-KEM/DEM: A New Framework for Hybrid Encryption and A New Analysis of Kurosawa-Desmedt KEM.* MIT Cryptography Seminar, January 2006.

13. *Multi-trapdoor Commitments and Their Applications to Proofs of Knowledge Secure Under Concurrent Man-in-the-Middle Attacks.* MIT Cryptography Seminar, November 2004; Ecole Normale Superieure, Paris, March 2004; U.C. Berkeley, Theory Seminar, Fall 2003; NYU Cryptography Seminar, Fall 2003; Stevens Institute of Technology, Fall 2003.

14. *A Framework for Password-Based Authenticated Key Exchange.* MIT Cryptography Seminar, Spring 2004; NYU Cryptography Seminar, Spring 2003.

15. *Lower bounds on the efficiency of encryption and digital signature schemes.* MIT Cryptography Seminar, Spring 2002.

16. *Braid Groups and Public Key Cryptography.* Dipartimento di Matematica e Informatica, Universita' di Catania, Italy, September 2001.

17. *Lower Bounds for Generic Cryptographic Constructions.* ETH Zurich, Monte Verita' Workshop on Cryptography, March 2001.

18. *Security for Multimedia Traffic over IP.* A five-lecture course at the Second International School on *Foundation of Security Analysis and Design*, September 17–29, 2001, Bertinoro, Italy, Sponsored by the EATCS (European Association for Theoretical Computer Science).

19. *Adaptive Security for Threshold Cryptosystems.* Ecole Normale Superieure, Luminy Workshop on Cryptography, September 1999.

20. *Secure Hash-and-Sign Signatures Without the Random Oracle.* IBM Almaden Research Center, January 1999.

21. *Cryptographic Primitives.* A five-lecture course at the 1998 International Summer School for Computer Science Researchers, July 5–18, 1998, Lipari, Italy.

22. *Simplified VSS and Fast-Track Multiparty Computation with Applications to Threshold Cryptography.* ETH Zurich, Monte Verita' Workshop on Cryptography, March 1998; Bell Labs, Crypto Seminar, June 1998.

23. *Secure Electronic Voting.* RSA Labs Seminars. August 1997.

24. *How to Sign Digital Streams.* Dipartimento di Informatica, Università di Torino. September 1997; DIMACS Research and Education Institute (DREI), Rutgers University, July 1997.

25. *Incoercible Multiparty Computation.* DIMACS Special Year on Networks, AT&T Labs, January 1997.

26. *Robust and Efficient Sharing of RSA Functions.* NYU Computer Science Colloquium. March 1996; IBM Research, Network Security Seminar Series. February 1996; MIT Cryptography Seminar, December 1995.

27. *Robust Threshold DSS Signatures.* RSA Labs, January 1996.

Conference Presentations

1. *Highly Scalable Verifiable Encrypted Search.* IEEE Workshop on Security and Privacy in the Cloud. Florence, Italy, September 2015.

2. *Making the Diffie-Hellman Protocol Identity-Based.* 2010 RSA Security Conference (Crypto Track), San Francisco, CA, March 2010.

3. *Strongly-Resilient and Non-interactive Hierarchical Key-Agreement in MANETs.* 2008 European Symposium on Research in Computer Security (ESORICS'08), Torremolinos, Spain, October 2008.

4. *Faster and Shorter Password-Authenticated Key Exchange.* 2008 Theory of Cryptography Conference (TCC'08), New York, February 2008.

5. *Deniable Authentication and Key Exchange.* 2006 ACM Conference on Computer and Communication Security (CCS'06), Alexandria VA, November 2006.

6. *Independent Zero-Knowledge Sets.* 2006 International Colloquium on Automata, Languages and Programming (ICALP'06), Venice, Italy, July 2006.

7. *New Approaches for Deniable Authentication.* 2005 ACM Conference on Computer and Communication Security (CCS'05), Alexandria VA, November 2005.

8. *The Security of "Off-the-Record Messaging".* 2005 ACM Workshop on Privacy in the Electronic Society, (WPES'05), Alexandria VA, November 2005.

9. *Tag-KEM/DEM: A New Framework for Hybrid Encryption and A New Analysis of Kurosawa-Desmedt KEM.* EUROCRYPT 2005, Aarhus, Denmark, May 2005.

10. *Batching Schnorr Identification Scheme with Applications to Privacy-Preserving Authorization and Low-Bandwidth Communication Devices.* ASIACRYPT 2004, Cheju, Korea, December 2004.

11. *Multi-trapdoor Commitments and Their Applications to Proofs of Knowledge Secure Under Concurrent Man-in-the-Middle Attacks.* CRYPTO 2004, Santa Barbara CA, August 2004.

12. *Lower bounds on the efficiency of encryption and digital signature schemes.* 2003 ACM Symposium on the Theory of Computing (STOC'03), San Diego CA, June 2003.

13. *Provably Secure Threshold Password-Authenticated Key Exchange.* EUROCRYPT 2003, Warsaw, Poland, May 2003.

14. *Cryptanalysis of a Pseudorandom Generator Based on Braid Groups.* EUROCRYPT 2002, Amsterdam, The Netherlands, May 2002.

15. *The Round Complexity of Verifiable Secret Sharing and Secure Multicast.* 2001 ACM Symposium on the Theory of Computing (STOC'01), Crete, Greece, July 2001.

16. *An Improved Pseudo-Random Generator Based on Discrete Log.* CRYPTO'2000, Santa Barbara CA. August 2000.

17. *Secure Distributed Storage and Retrieval.* 1999 RSA Conference, San Jose CA, January 1999.

18. *Simplified VSS and Fast-Track Multiparty Computation with Applications to Threshold Cryptography.* Seventeenth Annual ACM Symposium on Principles of Distributed Computation, (PODC 1998), Puerto Vallarta, Mexico, June 1998.

19. *Incoercible Multiparty Computation.* 1996 IEEE Symposium on the Foundations of Computer Science (FOCS 96), Burlington VT, October 1996.

20. *Robust and Efficient Sharing of RSA Functions.* CRYPTO'96, Santa Barbara CA, August 1996.

21. *Robust Threshold DSS Signatures.* EUROCRYPT'96, Zaragoza, Spain, May 1996.

22. *Achieving Independence Efficiently and Securely.* Fourteenth Annual Symposium on Principles of Distributed Computation (PODC'95), Ottawa, August 1995.

23. *Verifiable Secret Sharing as Secure Computation.* EUROCRYPT'95, Saint-Malo, France, May 1995.