Elenco delle pubblicazioni scientifiche di Massimiliano Sala

Pubblicazioni accademiche in senso ampio

Journal Papers:	**54**				
Conference Papers:	**27**				
Unpublished preprints:	**17**				
Scopus h-index:	**10**	--	Scopus citations:	**345**	
G. Scholar h-index:	**15**	--	G Scholar citations:	**820**	

Articoli su rivista

1. 2000 - coautore: A. Tamponi,
   A linear programming estimate of the weight distribution of BCH(255,k),
   IEEE Transactions on Information Theory, vol. 46, p. 2235--2237.
2. 2002,
   Groebner bases and distance of cyclic codes,
   Applicable Algebra in Engineering, Communication and Comput., vol. 13, p. 137--162.
3. 2003,
   Upper bounds on the dual distance of BCH(255,k),
   Design, Codes and Cryptography, vol. 30, p. 159--168.
4. 2003 - coautore: T. Mora,
   On the Groebner bases of some symmetric systems and their application to Coding Theory,
   Journal of Symbolic Computation, vol. 35, p. 177--194.
5. 2005 - coautore: E. Orsini,
   Correcting errors and erasures via the syndrome variety,
   Journal of Pure and Applied Algebra, vol. 200, p. 191--226.
6. 2005 - coautori: M. Giorgetti, M. Rossi
   On the Groebner basis of a family of quasi-cyclic LDPC codes,
   Bulletin of the Iranian Mathematical Society, vol. 31, p. 13--32.
7. 2006 - coautore: E. Betti
   A new bound for the minimum distance of a cyclic code from its defining set,
   IEEE Transactions on Information Theory, vol. 52, p. 3700--3706.
8. 2006 - coautori: A. Caranti, F. Dalla Volta
   Abelian regular subgroups of the affine group and radical rings,
   Publicationes Mathematicae Debrecen, vol. 69, p. 297--308.

9. 2007 - coautore: E. Orsini
   General error locator polynomials for binary cyclic codes,
   IEEE Transactions on Information Theory, vol. 53, p. 1095--1107.
10. 2007,
    Groebner basis techniques to compute weight distributions of shortened cyclic codes,
    Journal of Algebra and its Applications, vol. 6, p. 403--414.
11. 2009 - coautori: R. Agarwal, B. O'Flynn, E. Popovici
    Error Resilient Data Transport in Sensor Network Applications: A Generic Perspective,
    International Journal of Circuit Theory and Applications, vol. 37, p. 377--396.
12. 2009 - coautori: A. Caranti, F. Dalla Volta
    On some block ciphers and imprimitive groups,
    Applicable Algebra in Engineering, Communication and Computing, vol. 20, p. 339--350.
13. 2009 - coautore: M. Giorgetti
    A commutative algebra approach to linear codes,
    Journal of Algebra, vol. 321, no. 8, p. 2259--2286.
14. 2009 - coautori: A. Caranti, F. Dalla Volta
    An application of the O'Nan-Scott theorem to the group generated by the round functions of an AES-like cipher,
    Design, Codes and Cryptography, vol. 52, p. 293--301.
15. 2010 - coautori: E. Guerrini, E. Orsini
    Computing the distance distribution of systematic non-linear codes,
    Journal of Algebra and its Applications, 2010, vol. 9, p. 241--256.
16. 2011 - coautori: L. Maines, M. Piva, A. Rimoldi
    On the provable security of BEAR and LION schemes,
    Applicable Algebra in Engineering, Communication and Computing, vol. 22, p. 413--423.
17. 2012 - coautori: C. Fontanari, V. Pulice, A. Rimoldi
    On weakly APN functions and 4-bit S-Boxes,
    Finite Fields and their Applications, vol. 18, p. 522--528.
18. 2012 - coautori: E. Orsini, C. Marcolla
    Improved decoding of affine-variety codes,
    Journal of Pure and Applied Algebra, vol. 216, p. 1533--1565.
19. 2012 - coautori: E. Ballico, M. C. Brambilla, F. Caruso
    Postulation of general quintuple fat point schemes in P3,
    Journal of Algebra, vol. 363, p. 113--139.
20. 2013 - coautori: E. Ballico, M. Elia
    On the evaluation of multivariate polynomials over finite fields,
    Journal of Symbolic Computation, vol. 50, p. 255--262.

Elenco delle pubblicazioni scientifiche di Massimiliano Sala

---

21. 2014 - coautori: R. Aragona, A. Caranti, F. Dalla Volta
    On the group generated by the round functions of translation based ciphers over arbitrary finite fields,
    Finite Fields and their Applications, vol. 25, p. 293--305.
22. 2014 - coautori:,E. Bellini, E. Guerrini
    Some Bounds on the Size of Codes,
    IEEE Transactions on Information Theory, vol. 60, p. 1475--1480.
23. 2014 - coautori: C. Marcolla, M. Pellegrini
    On the Hermitian curve and its intersections with some conics,
    Finite Fields and their Applications, vol. 28, p. 166--187.
24. 2014 - coautori: R. Aragona, C. Marcolla, F. Marinelli
    Some security bounds for the key sizes of DGHV scheme,
    Applicable Algebra in Engineering, Communication and Computing, vol. 25, p.383--392.
25. 2016 - coautori: C. Marcolla, M. Pellegrini
    On the small weights codewords of some Hermitian codes,
    Journal of Symbolic Computation, vol. 73, p. 27--45.
26. 2016 - coautori: P. Peterlongo, C. Tinnirello
    A discrete logarithm-based approach to compute low-weight multiples of binary polynomials,
    Finite Fields and their Applications, vol. 38, p. 57--71.
27. 2016 - coautori: R. Aragona, M. Calderini, D. Maccauro
    On weak differential uniformity of vectorial Boolean functions as a cryptographic criterion,
    Applicable Algebra in Engineering, Communication and Computing, vol. 27, p. 359--372.
28. 2016 - coautori: E. Guerrini, A. Meneghetti
    On optimal nonlinear systematic codes,
    IEEE Transactions on Information Theory, vol. 62, p. 3103--3112.
29. 2016 - coautori: A. Meneghetti, A. Tomasi et al
    Generation of high quality random numbers via an all-silicon-based approach,
    Physica Status Solidi (A) Applications and Materials Science, vol. 213, p. 3186--3193.
30. 2017 - coautori: R. Aragona, A. Caranti
    The group generated by the round functions of a GOST-like cipher,
    Annali di Matematica Pura e Applicata, vol. 196, p. 1--17.
31. 2017 - coautori: R. Aragona, R. Longo
    Several proofs of security for a tokenization algorithm,
    Applicable Algebra in Engineering, Communication and Computing, vol. 28, p. 425--436.
32. 2017 - coautori: M. Calderini, I. Villa
    A note on APN permutations in even dimension,
    Finite Fields and Their Applications, vol. 46, p. 1--16.

Elenco delle pubblicazioni scientifiche di Massimiliano Sala

33. 2017 - coautori: A. Meneghetti, A. Tomasi
Code generator matrices as RNG conditioners,
Finite Fields and their Applications, vol. 47, p. 46--63.

34. 2017 - coautori: F. Caruso, E. Orsini, C. Tinnirello
On the shape of the general error locator polynomial for cyclic codes,
IEEE Transactions on Information Theory, vol. 63, p. 3641--3657.

35. 2018 - coautori: R. Aragona, A. Rimoldi
A note on an infeasible linearization of some block ciphers,
Journal of Discrete Mathematical Sciences and Cryptography, Vol. 21, p. 209--218.

36. 2018 - coautori: A. Amadori, F. Pintore
On the discrete logarithm problem for prime-field elliptic curves,
Finite Fields and their Applications, vol. 51, p. 168--182.

37. 2018 - coautori: C. Mascia, G. Rinaldo
Hilbert quasi-polynomials for order domains and applications to coding theory,
Advances in Mathematics of Communications, vol. 12, p. 287--301.

38. 2018 - coautori: R. Aragona, F. Giacon
A proof of security for a key-policy RS-ABE scheme,
JP Journal of Algebra, Number Theory and Applications, vol. 40, p. 29--90.

39. 2018 - coautore: E. Bellini
A deterministic algorithm for the distance and weight distribution of binary nonlinear codes,
International Journal of Information and Coding Theory, vol. 5, p. 18--35.

40. 2019 - coautore: M. Calderini
On Hidden Sums Compatible with A Given Block Cipher Diffusion Layer,
Discrete Mathematics, vol. 342, p. 373--386.

41. 2019 - coautori: R. Aragona, M. Calderini, R. Civino, I. Zappatore
Wave-shaped round functions and primitive groups,
Advances in Mathematics of Communications, vol. 13, p. 67--88.

42. 2019 - coautori: A. Meneghetti, A.O. Quintavalle, A. Tomasi
Two-tier blockchain timestamped notarization with incremental security,
Annals of Emerging Technologies in Computing, vol. 3, p. 25--33.

43. 2019 - coautore: M. Pellegrini
Weight distribution of Hermitian codes and matrices rank,
Finite Fields and their Applications, vol. 60, art. 101578.

44. 2019 - coautori: A. Meneghetti, T. Parise, D. Taufer
A survey on efficient parallelization of blockchain-based smart contracts,
Annals of Emerging Technologies in Computing, vol. 3, p. 9--16.

Elenco delle pubblicazioni scientifiche di Massimiliano Sala

45. 2019 - coautori: C. Blondeau, R. Civino
Differential attacks: using alternative operations,
Designs, Codes, and Cryptography, vol. 87, p. 225--247.

46. 2019 - coautori: C. Brunetta, M. Calderini
On hidden sums compatible with a given block cipher diffusion layer,
Discrete Mathematics, vol. 342, p. 373--386.

47. 2020 - coautori: M. Ceria, T. Mora
Zech tableaux as tools for sparse decoding,
Rendiconti Sem. Mat. Univ. Pol. Torino, vol. 78, p. 43 -- 56.

48. 2020 - coautore: M. Bonini
Intersections between the norm-trace curve and some low degree curves,
Finite Fields and their Applications, vol. 67, art. 101715.

49. 2020 - coautori: D. Sogiorno, D. Taufer
A small subgroup attack on Bitcoin address generation,
Mathematics, vol. 8, art. 1645.

50. 2020 - coautore: A. Musukwa
On the linear structures of balanced functions and quadratic APN functions,
Cryptography and Communications, vol. 12, p. 859--880.

51. 2020 - coautori: M. Ceria, T. Mora
HELP: a sparse error locator polynomial for BCH codes,
Applicable Algebra in Engineering, Communications and Computing, vol. 31, p. 215-233.

52. 2020 - coautori: A. Meneghetti, D. Taufer
A new ECDLP-based PoW model,
Mathematics, vol. 8, art. 1344.

53. 2020 - coautori: A. Meneghetti, D. Taufer
A survey on PoW-based consensus,
Annals of Emerging Technologies in Computing, vol. 4, p. 8--18.

54. 2020 - coautori: R. Civino, M. Calderini
On properties of translation groups in the affine general linear group with applications to cryptography,
Journal of Algebra. accepted for publication,
DOI: 10.1016/j.jalgebra.2020.10.034