Cascudo, Ignacio; **Cramer, Ronald**; **Mirandola, Diego**; **Padró, Carles**; **Xing, Chaoping**
On secret sharing with nonlinear product reconstruction. (English) Zbl 1397.94113
SIAM J. Discrete Math. 29, No. 2, 1114-1131 (2015).

MSC:

94A62 Authentication, digital signatures and secret sharing
94A60 Cryptography

Keywords:

(arithmetic) secret sharing

Full Text: DOI

References:

[1] N. Bourbaki, \textit{Algebra} I, Springer-Verlag, New York, 1989.

[2] M. Ben-Or, S. Goldwasser, and A. Wigderson, \textit{Completeness theorems for non-cryptographic fault-tolerant distributed computation}, in Proceedings of STOC 1988, ACM Press, New York, 1988, pp. 1–10.

[3] I. Cascudo, H. Chen, R. Cramer, and C. Xing, \textit{Asymptotically good ideal linear secret sharing with strong multiplication over \textit{any} fixed finite field}, in Proceedings of the 29th Annual IACR CRYPTO, Santa Barbara, CA, Lecture Notes in Comput. Sci. 5677, Springer-Verlag, New York, 2009, pp. 466–486. · Zbl 1252.94106

[4] I. Cascudo, R. Cramer, and C. Xing, \textit{The torsion-limit for algebraic function fields and its application to arithmetic secret sharing}, in Proceedings of the of 31st Annual IACR CRYPTO, Santa Barbara, CA, Lecture Notes in Comput. Sci. 6842, Springer-Verlag, New York, 2011, pp. 685–705. · Zbl 1290.94148

[5] D. Chaum, C. Crépeau, and I. Damgaard, \textit{Multi-party unconditionally secure protocols}, in Proceedings of STOC 1988, ACM Press, New York, 1988, pp. 11–19.

[6] H. Chen and R. Cramer, \textit{Algebraic geometric secret sharing schemes and secure multi-party computation over small fields}, in Proceedings of the 26th Annual IACR CRYPTO, Santa Barbara, CA, Lecture Notes in Comput. Sci. 4117, Springer-Verlag, New York, 2006, pp. 516–531. · Zbl 1129.94016

[7] H. Chen, R. Cramer, S. Goldwasser, R. de Haan, and V. Vaikuntanathan, \textit{Secure computation from random error correcting codes}, in Proceedings of the 27th Annual IACR EUROCRYPT, Barcelona, Spain, Lecture Notes in Comput. Sci. 4515, Springer-Verlag, New York, 2007, pp. 291–310. · Zbl 1141.94346

[8] R. Cramer, I. Damg\rard, and U. Maurer, \textit{General secure multi-party computation from any linear secret sharing scheme}, in Proceedings of 19th Annual IACR EUROCRYPT, Brugge, Belgium, Lecture Notes in Comput. Sci. 1807, Springer-Verlag, New York, 2000, pp. 316–334. · Zbl 1082.94515

[9] J. Dieudonné, \textit{La Géométrie des Groupes Classiques}, 2nd ed., Springer-Verlag, New York, 1963.

[10] R. H. Dye, \textit{On the Arf invariant}, J. Algebra, 53 (1978), pp. 36–39. · Zbl 0393.10019

[11] M. K. Franklin and M. Yung, \textit{Communication complexity of secure computation (extended abstract)}, in Proceedings of STOC 1992, ACM Press, New York, 1992, pp. 699–710.

[12] Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai, \textit{Zero-knowledge from secure multiparty computation}, in Proceedings of 39th STOC, San Diego, CA, ACM Press, New York, 2007, pp. 21–30. · Zbl 1232.68044

[13] T. Y. Lam, \textit{Introduction to Quadratic Forms over Fields}. Grad. Stud. Math. 67, AMS, Providence, RI, 2005. · Zbl 1068.11023

[14] S. Roman, \textit{Advanced Linear Algebra}, 3rd ed., Springer-Verlag, New York, 2008. · Zbl 1132.15002

[15] J.-P. Serre, \textit{A course in arithmetic}, Grad. Texts in Math. 7, Springer-Verlag, New York, 1973.

[16] A. Shamir, \textit{How to share a secret}, Comm. ACM, 22 (1979), pp. 612–613. · Zbl 0414.94021