Brakerski, Zvika; **Gentry, Craig**; **Vaikuntanathan, Vinod**

(Leveled) fully homomorphic encryption without bootstrapping. (English) Zbl 1347.68120

Proceedings of the 3rd conference on innovations in theoretical computer science, ITCS'12, Cambridge, MA, USA, January 8–10, 2012. New York, NY: Association for Computing Machinery (ACM) (ISBN 978-1-4503-1115-1). 309-325 (2012).

MSC:

68P25 Data encryption (aspects in computer science)
94A60 Cryptography

Keywords:

bootstrapping; fully homomorphic encryption; learning with errors; modulus reduction

Full Text: DOI

References:

[1] K. B. Athreya, J. M. Hitchcock, J. H. Lutz, and E. Mayordomo. E.ective strong dimension in algorithmic information and computational complexity. SIAM Journal on Computing, 37(3):671 705, 2007. · Zbl 1144.68029

[2] P. Billingsley. Ergodic Theory and Information. John Wiley and Sons, 1965. · Zbl 0141.16702

[3] C.-L. Chang and Y.-D. Lyuu. E.cient testing of forecasts. International Journal of Foundations of Computer Science, 21(1):61 72, 2010.

[4] A. Dawid. The well-calibrated Bayesian. Journal of the American Statistical Association, 77(379):605 610, 1982. · Zbl 0495.62005

[5] H. Eggleston. The fractional dimension of a set de.ned by decimal properties. Quarterly Journal of Mathematics, 20:31 36, 1949. · Zbl 0031.20801

[6] L. Fortnow and R. V. Vohra. The complexity of forecast testing. Econometrica, 77:93 105, 2009. · Zbl 1160.91396

[7] D. P. Foster and R. V. Vohra. Asymptotic calibration. Biometrika, 85(2):379 390, 1998. · Zbl 0947.62059

[8] L. A. Hemaspaandra. Sigact news complexity theory column 48. SIGACT News, 36(3):24 38, 2005. Guest Column: The Fractal Geometry of Complexity Classes, by J. M. Hitchcock, J. H. Lutz, and E. Mayordomo.

[9] J. H. Lutz. Dimension in complexity classes. SIAM Journal on Computing, 32(5):1236 1259, 2003. · Zbl 1026.68059

[10] J. H. Lutz. The dimensions of individual strings and sequences. Information and Computation, 187(1):49 79, 2003. · Zbl 1090.68053

[11] N. Merhav and M. Feder. Universal prediction. IEEE Transactions on Information Theory, 44(6):2124 2147, 1998. · Zbl 0933.94008

[12] A. Sandroni. The reproducible properties of correct forecasts. International Journal of Game Theory, 32(1):151 159, December 2003. · Zbl 1071.62084