

**Nissim, Kobbi; Vadhan, Salil; Xiao, David**

**Redrawing the boundaries on purchasing data from privacy-sensitive individuals.** (English)

[Zbl 1366.91094](#)

Proceedings of the 5th conference on innovations in theoretical computer science, ITCS'14, Princeton, NJ, USA, January 11–14, 2014. New York, NY: Association for Computing Machinery (ACM) (ISBN 978-1-4503-2243-0). 411-421 (2014).

**MSC:**

[91B26](#) Auctions, bargaining, bidding and selling, and other market models  
[94A62](#) Authentication, digital signatures and secret sharing

Cited in **2** Documents

**Keywords:**

[differential privacy](#); [mechanism design](#)

**Full Text:** [DOI](#)

**References:**

- [1] M. Ajtai and C. Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In F. T. Leighton and P. W. Shor, editors, STOC, pages 284–293. ACM, 1997. · [Zbl 0962.68055](#)
- [2] D. A. M. Barrington. Bounded-width polynomial-size branching programs recognize exactly those languages in  $nc^1$ . J. Comput. Syst. Sci., 38(1):150–164, 1989. · [Zbl 0667.68059](#)
- [3] A. Borodin, D. Dolev, F. E. Fich, and W. J. Paul. Bounds for width two branching programs. SIAM J. Comput., 15(2):549–560, 1986. · [Zbl 0589.68034](#)
- [4] Z. Brakerski. Fully homomorphic encryption without modulus switching from classical GapSVP. In R. Safavi-Naini and R. Canetti, editors, CRYPTO, volume 7417 of Lecture Notes in Computer Science, pages 868–886. Springer, 2012. · [Zbl 1296.94091](#)
- [5] Z. Brakerski, C. Gentry, and V. Vaikuntanathan. (Leveled) fully homomorphic encryption without bootstrapping. In S. Goldwasser, editor, ITCS, pages 309–325. ACM, 2012. Invited to ACM Transactions on Computation Theory. · [Zbl 1347.68120](#)
- [6] Z. Brakerski, A. Langlois, C. Peikert, O. Regev, and D. Stehlé. Classical hardness of learning with errors. CoRR, abs/1306.0281, 2013. Preliminary version in STOC 2013.
- [7] Z. Brakerski and V. Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. In R. Ostrovsky, editor, FOCS, pages 97–106. IEEE, 2011. Invited to SIAM Journal on Computing. · [Zbl 1292.94038](#)
- [8] C. Gentry. A fully homomorphic encryption scheme. PhD thesis, Stanford University, 2009. · [Zbl 1304.94059](#)
- [9] C. Gentry. Fully homomorphic encryption using ideal lattices. In STOC, pages 169–178, 2009. · [Zbl 1304.94059](#)
- [10] C. Gentry. Toward basing fully homomorphic encryption on worst-case hardness. In CRYPTO, pages 116–137, 2010. · [Zbl 1280.94059](#)
- [11] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In C. Dwork, editor, STOC, pages 197–206. ACM, 2008. · [Zbl 1231.68124](#)
- [12] C. Gentry, A. Sahai, and B. Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. IACR Cryptology ePrint Archive, 2013:340, 2013. Preliminary version in CRYPTO 2013. · [Zbl 1310.94148](#)
- [13] Y. Ishai and A. Paskin. Evaluating branching programs on encrypted data. In S. P. Vadhan, editor, TCC, volume 4392 of Lecture Notes in Computer Science, pages 575–594. Springer, 2007. · [Zbl 1156.94354](#)
- [14] D. Micciancio and P. Mol. Pseudorandom knapsacks and the sample complexity of lwe search-to-decision reductions. In P. Rogaway, editor, CRYPTO, volume 6841 of Lecture Notes in Computer Science, pages 465–484. Springer, 2011. · [Zbl 1287.94085](#)
- [15] D. Micciancio and C. Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. IACR Cryptology ePrint Archive, 2011:501, 2011. Extended abstract in Eurocrypt 2012. · [Zbl 1297.94090](#)
- [16] C. Peikert. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In M. Mitzenmacher, editor, STOC, pages 333–342. ACM, 2009. · [Zbl 1304.94079](#)
- [17] O. Regev. New lattice-based cryptographic constructions. J. ACM, 51(6):899–942, 2004. · [Zbl 1125.94026](#)
- [18] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In H. N. Gabow and R. Fagin, editors, STOC, pages 84–93. ACM, 2005. Full version in · [Zbl 1192.94106](#)

19

- [19] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6), 2009. · [Zbl 1325.68101](#)
- [20] C.-P. Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. *Theor. Comput. Sci.*, 53:201–224, 1987. · [Zbl 0642.10030](#)

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.