[1] L. Ballard, S. Kamara, and F. Monrose, “Achieving efficient conjunctive keyword searches over encrypted data,” in Proc. of ICICS’05. Springer, 2005, pp. 414–426.

[2] R. Bost, “Po'o&: Forward secure searchable encryption,” in Proc. Of CCS’16. ACM, 2016, pp. 1143–1154.

[3] R. Bost, B. Minaud, and O. Ohrimenko, “Forward and backward private searchable encryption from constrained cryptographic primitives,” in

Proc. of CCS’17. ACM, 2017, pp. 1465–1482.

[4] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy-preserving multi-keyword ranked search over encrypted cloud data,” IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 1, pp. 222–233, 2014.

[5] D. Cash, J. Jaeger, S. Jarecki, C. S. Jutla, H. Krawczyk, M.-C. Rosu, and M. Steiner, “Dynamic searchable encryption in very-large databases: Data structures and implementation,” in Proc. of NDSS’14, 2014.

[6] D. Cash, S. Jarecki, C. S. Jutla, H. Krawczyk, M.-C. Rosu, and M. Steiner, “Highly-scalable searchable symmetric encryption with support for boolean queries,” in Proc. of CRYPTO’13. Springer, 2013,

pp. 353–373.

[7] Y. Chang and M. Mitzenmacher, “Privacy preserving keyword searches on remote encrypted data,” in Proc. of ACNS’05. Springer, 2005, pp. 442–455.

[8] M. Chase and S. Kamara, “Structured encryption and controlled disclosure,” in Proc. of ASIACRYPT’10. Springer, 2010, pp. 577–594.

[9] R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: Improved definitions and efficient constructions,” in Proc. of CCS’06. ACM, 2006, pp. 79–88.

[10] E.-J. Goh et al., “Secure indexes.” IACR Cryptology ePrint Archive, vol.

2003, p. 216, 2003.

[11] P. Golle, J. Staddon, and B. Waters, “Secure conjunctive keyword search

over encrypted data,” in Proc. of ACNS’04. Springer, 2004, pp. 31–45.

[12] F. Hahn and F. Kerschbaum, “Searchable encryption with secure and efficient updates,” in Proc. of CCS’14. ACM, 2014, pp. 310–320.

[13] K. He, J. Chen, R. Du, Q. Wu, G. Xue, and X. Zhang, “Deypos: Deduplicatable dynamic proof of storage for multi-user environments,” IEEE Transactions on Computers, vol. 65, no. 12, pp. 3631–3645, 2016.]

[14] S. Hu, Q. Wang, J. Wang, Z. Qin, and K. Ren, “Securing sift: Privacy-preserving outsourcing computation of feature extractions over encrypted image data,” IEEE Trans. on Image Processing, vol. 25, no. 7,

pp. 3411–3425, 2016.

[15] S. Kamara and T. Moataz, “Boolean searchable symmetric encryption

with worst-case sub-linear complexity,” in Proc. of EUROCRYPT’17.  
Springer, 2017, pp. 94–124.

[16] S. Kamara and C. Papamanthou, “Parallel and dynamic searchable

symmetric encryption,” in Proc. of FC’13. Springer, 2013, pp. 258–274.

[17] S. Kamara, C. Papamanthou, and T. Roeder, “Dynamic searchable symmetric encryption,” in Proc. of CCS’12. ACM, 2012, pp. 965–

976.

[18] J. Katz and Y. Lindell, Introduction to modern cryptography. CRC

press, 2014.

[19] K. S. Kim, M. Kim, D. Lee, J. H. Park, and W.-H. Kim, “Forward

secure dynamic searchable symmetric encryption with efficient updates,”

in Proc. of CCS’17. ACM, 2017, pp. 1449–1463.

[20] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, “Fuzzy

keyword search over encrypted data in cloud computing,” in Proc. of

INFOCOM’10. IEEE, 2010, pp. 441–445.

[21] T. Moataz and A. Shikfa, “Boolean symmetric searchable encryption,”

in Proc. of AsiaCCS’13. ACM, 2013, pp. 265–276.

[22] P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” in Proc. of EUROCRYPT’99. Springer, 1999, pp. 223–

238.

[23] V. Pappas, F. Krell, B. Vo, V. Kolesnikov, T. Malkin, S. G. Choi,

W. George, A. Keromytis, and S. Bellovin, “Blind seer: A scalable

private DBMS,” in Proc. of S&P’14. IEEE, 2014, pp. 359–374.

[24] J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, “An efficient public

auditing protocol with novel dynamic structure for cloud data,” IEEE

Transactions on Information Forensics and Security, vol. 12, no. 10, pp.

2402–2415, 2017.

[25] D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searches

on encrypted data,” in Proc. of S&P’00. IEEE, 2000, pp. 44–55.

[26] E. Stefanov, C. Papamanthou, and E. Shi, “Practical dynamic searchable

encryption with small leakage,” in Proc. of NDSS’14, 2014, pp. 23–26.

[27] B. Wang, S. Yu, W. Lou, and Y. T. Hou, “Privacy-preserving multikeyword fuzzy search over encrypted data in the cloud,” in Proc. Of INFOCOM’14. IEEE, pp. 2112–2120.

[28] C. Wang, K. Ren, J. Wang, and Q. Wang, “Harnessing the cloud for securely outsourcing large-scale systems of linear equations,” IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 1172–1181, 2013.

[29] Q. Wang, M. He, M. Du, S. S. M. Chow, R. W. F. Lai, and Q. Zou, “Searchable encryption over feature-rich data,” IEEE Transactions on Dependable and Secure Computing, vol. PP, pp. 1–1, DOI: 10.1109/TDSC.2016.2 593 444, 2016.

[30] Q. Wang, S. Hu, K. Ren, M. He, M. Du, and Z. Wang, “Cloudbi: Practical privacy-preserving outsourcing of biometric identification in the cloud,” in Proc. of ESORICS’2015. Springer, 2015, pp. 186–205.

[31] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, “Enabling publicauditability and data dynamics for storage security in cloud computing,”

IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 5, pp. 847–859, 2011.

[32] W. K. Wong, D. W.-L. Cheung, B. Kao, and N. Mamoulis, “Secure knn

computation on encrypted databases,” in Proc. Of SIGMOD’09. ACM,

2009, pp. 139–152.

[33] Y. Zhang, J. Katz, and C. Papamanthou, “All your queries are belong to us: The power of file-injection attacks on searchable encryption,” in

Proc. of USENIX Security’16, 2016, pp. 707–720.