**REFERENCES**

* C. Dong, L. Chen, and Z. Wen, “When private set intersection meets big data: an efficient and scalable protocol,” in Proc. of CCS’13. ACM, 2013, pp. 789–800.
* K. Yang, X. Jia, and K. Ren, “Secure and verifiable policy update outsourcing for big data access control in the cloud,” IEEE Trans.
* Parallel Distrib. Syst., vol. 26, no. 12, pp. 3461–3470, Dec 2015.
* J. Hur, “Attribute-based secure data sharing with hidden policies in smart grid,” IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 11, pp. 2171–2180, 2013.
* P. Mell and T. Grance, “The NIST definition of cloud computing,” [Recommendations of the National Institute of Standards and Technology- Special Publication 800-145], 2011.
* [2] R. Lu, H. Zhu, X. Liu, J. K. Liu, and J. Shao, “Toward efficient and privacy-preserving computing in big data era,” IEEE Network, vol. 28, no. 4, pp. 46–50, 2014.
* [3] K. Yang and X. Jia, “Expressive, efficient, and revocable data access control for multi-authority cloud storage,” IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 7, pp. 1735–1744, July 2014.
* [4] H. Li, D. Liu, K. Alharbi, S. Zhang, and X. Lin, “Enabling fine-grained access control with efficient attribute revocation and policy updating in smart grid,” KSII Transactions on Internet and Information Systems (TIIS), vol. 9, no. 4, pp. 1404–1423, 2015.
* [5] K. Yang, Z. Liu, X. Jia, and X. S. Shen, “Time-domain attribute-based access control for cloud-based video content sharing: A cryptographic approach,” IEEE Trans. on Multimedia (to appear), February 2016.
* [6] B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in Proc. of PKC’11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 53–70.
* [7] H. Lin, Z. Cao, X. Liang, and J. Shao, “Secure threshold multi authority attribute based encryption without a central authority,” in Proc. Of INDOCRYPT’08. Springer, 2008, pp. 426–436.
* [8] T. Nishide, K. Yoneyama, and K. Ohta, “Attribute-based encryption with partially hidden encryptor-specified access structures,” in Applied cryptography and network security. Springer, 2008, pp. 111–129.
* [9] J. Li, K. Ren, B. Zhu, and Z. Wan, “Privacy-aware attribute-based encryption with user accountability,” in Information Security. Springer, 2009, pp. 347–362.
* [10] D. Boneh and B. Waters, “Conjunctive, subset, and range queries on encrypted data,” in Theory of cryptography. Springer, 2007, pp. 535– 554.
* [11] J. Katz, A. Sahai, and B. Waters, “Predicate encryption supporting disjunctions, polynomial equations, and inner products,” in Advances in Cryptology–EUROCRYPT’08. Springer, 2008, pp. 146–162.
* [12] J. Lai, R. H. Deng, and Y. Li, “Fully secure cipertext-policy hiding cpabe,” in Information Security Practice and Experience. Springer, 2011, pp. 24–39.
* [13] L. Lei, Z. Zhong, K. Zheng, J. Chen, and H. Meng, “Challenges on wireless heterogeneous networks for mobile cloud computing,” IEEE Wireless Communications, vol. 20, no. 3, pp. 34–44, 2013.
* [14] K. Zheng, Z. Yang, K. Zhang, P. Chatzimisios, K. Yang, and W. Xiang, “Big data-driven optimization for mobile networks toward 5g,” IEEE Network, vol. 30, no. 1, pp. 44–51, 2016.
* [15] Z. Su, Q. Xu, and Q. Qi, “Big data in mobile social networks: a qoeoriented framework,” IEEE Network, vol. 30, no. 1, pp. 52–57, 2016.
* [16] H. Li, D. Liu, Y. Dai, and T. H. Luan, “Engineering searchable encryption of mobile cloud networks: when qoe meets qop,” IEEE
* Wireless Communications, vol. 22, no. 4, pp. 74–80, 2015.