**REFERENCES**

[1] C. Wang, N. Cao, J. Li, K. Ren, W. Lou. “Secure ranked keyword search over encrypted cloud data”[C]//IEEE 30th International Conference on Distributed Computing Systems (ICDCS), IEEE, 2010: 253-262.

[2] Q. Zhang, L. T. Yang, Z. Chen, P. Li, M. J. Deen. “Privacy-preserving Double-Projection Deep Computation Model with Crowd sourcing on Cloud for Big Data Feature Learning,” IEEE Internet of Things Journal, 2017, DOI: 10.1109/JIOT.2017.2732735.

[3] R. Chen, Y. Mu, G. Yang, F. Guo and X. Wang, “Dual-Server Public- Key Encryption with Keyword Search for Secure Cloud Storage,” IEEE Transactions on Information Forensics and Security, 2016, vol.11, no. 4, 789-798.

[4] X. Liu, R.H. Deng, K.K.R. Choo, J. Weng. ”An efficient privacypreserving

outsourced calculation toolkit with multiple keys.” IEEE Transactions on Information Forensics and Security 11.11 (2016): 2401-2414.

[5] B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, “Building an encrypted and searchable audit log,” in NDSS, 2004.

[6] Y. Yang, X. Liu, R.H. Deng, “Multi-user Multi-Keyword Rank Search over Encrypted Data in Arbitrary Language”. IEEE Transactions on Dependable and Secure Computing, 2018, publish online, DOI: 10.1109/TDSC.2017.2787588.

[7] W. Sun, S. Yu, W. Lou, Y. Hou and H. Li, “Protecting Your Right: Verifiable Attribute-based Keyword Search with Finegrained Owner-enforced Search Authorization in the Cloud,” IEEE Transactions on Parallel and Distributed Systems, 2016, vol. 27, no.4, pp. 1187-1198.

[8] K. Liang, W. Susilo, “Searchable Attribute-Based Mechanism with Efficient Data Sharing for Secure Cloud Storage,” IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 9, pp. 1981-1992.

[9] M. Green, S. Hohenberger, and B.Waters, “Outsourcing the decryption of ABE ciphertexts,” in USENIX Security Symposium, ACM, 2011, pp. 34-34.

[10] J. Lai, R. H. Deng, C. Guan, and J. Weng, “Attribute-based encryption with verifiable outsourced decryption,” IEEE Transactions on Information Forensics and Security, 2013, vol. 8, no. 8, pp. 1343-1354.

[11] B. Qin, R. H. Deng, S. Liu, and S. Ma, “Attribute-Based Encryption with Efficient Verifiable Outsourced Decryption,” IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 7, pp. 1384-1394.

[12] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in: EUROCRYPT, 2004, pp.506-522.

[13] Z. Liu, Z. Cao, D.S. Wong, “White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures,” IEEE Transactions on Information Forensics and Security,2013, vol. 8, no. 1, pp. 76-88.

[14] J. Ning, X. Dong, Z. Cao, L. Wei, X. Lin, “White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Flexible Attributes,” IEEE Transactions on Information Forensics and Security,2015, vol. 10, no. 6, pp. 1274-1288.

[15] Z. Liu, Z. Cao, D.S. Wong, “Traceable CP-ABE: how to trace decryption devices found in the wild,” IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 1, pp. 55-68.

[16] D. Boneh and B. Waters, “Conjunctive, subset, and range queries on encrypted data,” in: 4th Theory Cryptogrophy Confonference, 2007, vol. 4392, pp. 535-554.

[17] P. Xu, H. Jin, Q. Wu and W. Wang, “Public-Key Encryption with Fuzzy Keyword Search: A Provably Secure Scheme under Keyword Gusssing Attack,” IEEE Transactions on Computers, 2013, vol. 62, no. 11, 2266-2277.

[18] Q. Tang, “Nothing is for Free: Security in Searching Shared and Encrypted Data,” IEEE Transactions on Information Forensics and Security, 2014, vol. 9, no. 11, 1943-1952.

[19] Y. Yang and M. Ma, “Conjunctive Keyword Search With Designated Tester and Timing Enabled Proxy Re-Encryption Function for E-Health Clouds,” IEEE Transactions on Information Forensics and Security, 2016, vol. 11, no. 4, 746-759.

[20] B. Zhang, F. Zhang, “An efficient public key encryption with conjunctive-subset keywords search,” Journal of Network and Computer Applications, 2011, vol. 34, no. 1, pp. 262-267.

[21] X. Wang, X. Huang, X. Yang, L. Liu, X. Wu, “Further observation on proxy re-encryption with keyword search,” Journal of Systems and Software, 2012, vol. 85, no. 3, pp. 643-654. 2168-7161 (c) 2018 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications\_standards/publications/rights/index.html for more information. This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCC.2018.2820714, IEEE Transactions on Cloud Computing IEEE TRANSACTIONS ON CLOUD COMPUTING 14

[22] L. Fang, W. Susilo, C. Ge, J. Wang, “Public key encryption with keyword search secure against keyword guessing attacks without random oracle,” Information Sciences, 2013, vol. 238, pp. 221-241.

[23] A. Sahai, B.Waters, “Fuzzy identity-based encryption,” in: EUROCRYPT,

Springer, 2005, vol. 3494, pp. 457-473.

[24] J. Han, W. Susilo, Y. Mu. “Improving Privacy and Security in Decentralized Ciphertext-Policy Attribute-Based Encryption,” IEEE Transactions on on Information Forensics and Security, 2015, vol. 10, no. 3, 665-678.

[25] Y. Shi, Q. Zheng, J. Liu. “Directly revocable key-policy attributebased encryption with verifiable ciphertext delegation,” Information Sciences, 2015, vol. 295, pp. 221-231.

[26] X. Mao, J. Lai, Q. Mei, K. Chen and J.Weng, “Generic and Efficient Constructions of Attribute-Based Encryption with Verifiable Outsourced Decryption,” IEEE Transactions on Dependable and Secure Computing, publish online, DOI: 10.1109/TDSC.2015.2423669.

[27] R. Ostrovsky, A. Sahai, B. Waters, “Attribute-based encryption with nonmonotonic access structures,” in: 14th ACM Conference on Computer and Communications Security, ACM, 2007, pp. 195- 203.

[28] C. Wang, J. Luo, “A key-policy attribute-based encryption scheme with constant size ciphertext,” in: 8th International Conference on Computational Intelligence and Security, 2012, pp. 447-451.

[29] C. Chen, Z. Zhang, and D. Feng, “Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost,” In: 5th International Conference on Provable Security, Springer, 2011, pp. 84-101.

[30] S. Hohenberger, B. Waters, “Attribute-based encryption with fast decryption,” in: PKC, springer, 2013, vol. 7778, pp. 162-179.

[31] D. Nishant, J. Devesh, “Fully secure ciphertext policy attributebased

encryption with constant length ciphertext and faster decryption,” Security and Communication Networks, 2014, vol. 7, no. 11, pp. 1988-2002.

[32] A. Lewko and B. Waters, “Decentralizing attribute-based encryption,”

in CRYPTO, Springer, 2011, vol. 6632, pp. 568-588.

[33] W. Guo, J. Li, G. Chen, Y. Niu, C. Chen, “A PSO-Optimized Realtime

Fault-tolerant Task Allocation Algorithm in Wireless Sensor Networks,” IEEE Transactions on Parallel and Distributed Systems, 2015, 26(12), pp. 3236-3249.

[34] W. Guo, J. Chen, G. Chen, H. Zheng, “Trust Dynamic Task Allocation Algorithm with Nash Equilibrium for Heterogeneous Wireless Sensor Network,” Security and Communication Networks, 2015, 8(10). pp. 1865-1877.

[35] C. Wang, N. Cao, K. Ren, W. Lou. “Enabling secure and efficient

ranked keyword search over outsourced cloud data,” IEEE Transactions

on parallel and distributed systems, 2012, 23(8): 1467-1479.

[36] N. Cao, C. Wang, M. Li, K. Ren, W. Lou. “Privacy-preserving

multi-keyword ranked search over encrypted cloud data,” IEEE

Transactions on parallel and distributed systems, 2014, 25(1): 222-

233.

[37] B. Chor, A. Fiat, and M. Naor. “Tracing traitors”. In: CRYPTO,

Springer, 1994, pp. 257-270.

[38] Z. Zhou, D. Huang, and Z. Wang. “Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption.” IEEE Transactions on Computers, 2015, vol. 64, no.1, pp. 126-138.

[39] J. Kim, W. Susilo, M. Au and J. Seberry, “Adaptively secure

identity-based broadcast encryption with a constant-sized ciphertext,”

IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 3, pp. 679-693.

[40] D. Hofheinz, C. Striecks, “A generic view on trace-and-revoke

broadcast encryption schemes,” In: CT-RSA, Springer, 2014, pp. 48-

63.

[41] A. Beimel. “Secure Schemes for Secret Sharing and Key Distribution”.

PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

[42] D. Boneh and X. Boyen, “Short signatures without random oracles,”

in: CRYPTO, Springer, 2004, vol. 3027, pp. 56-73.

[43] B. Waters, “Ciphertext-policy attribute-based encryption: An expressive,

efficient, and provably secure realization,” in: PKC, Springer, 2011, vol. 6571, pp. 53-70.

[44] B. Lynn. “The Stanford Pairing Based Crypto Library.” [Online] Available: http://crypto.stanford.edu/pbc, accessed May 7, 2014.

[45] M. Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, “Fully Homomorphic Encryption over the Integers,” In: EUROCRYPT, 2010, pp. 24-43.