[53] Orlandi C, Piva A, Barni M. Oblivious neural network computing via homomorphic encryption. EURASIP Journal on Information Security, 2007,2007(1):1–11. [doi: 10.1155/2007/37343]

[54] Gilad-Bachrach R, Dowlin N, Laine K, Lauter K, Naehrig M, Wernsing J. Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy. In: Proc. of the 33rd Int'l Conf. on Machine Learning. New York: IMLS, 2016. 201–210.

[55] Chabanne H, De Wargny A, Milgram J, Morel C, Prouff E. Privacy-preserving classification on deep neural network. IACR Cryptology ePrint Archive, 2017,2017:35.

[56] Hesamifard E, Takabi H, Ghasemi M. CryptoDL: Deep neural networks over encrypted data. arXiv Preprint arXiv:171105189, 2017.

[57] Phan NH, Wu XT, Dou DJ. Preserving differential privacy in convolutional deep belief networks. Machine Learning, 2017,106 (9-10):1681–1704. [doi: 10.1007/s10994-017-5656-2]

[58] Huang K, Liu X, Fu S, Guo D, Xu M. A lightweight privacy-preserving CNN feature extraction framework for mobile sensing. IEEE Trans. on Dependable and Secure Computing, 2019. [doi: 10.1109/TDSC.2019.2913362]

[59] Ma Z, Liu Y, Liu X, Ma J, Li F. Privacy-preserving outsourced speech recognition for smart IoT devices. IEEE Internet of Things Journal, 2019,6(5):8406–8420. [doi: 10.1109/JIOT.2019.2917933]

[60] Papernot N, Abadi M, Erlingsson U, Goodfellow I, Talwar K. Semi-supervised knowledge transfer for deep learning from private training data. arXiv Preprint arXiv:161005755, 2016.

[61] Vaidya J, Clifton C. Privacy-preserving *k*-means clustering over vertically partitioned data. In: Proc. of the 9th ACM SIGKDD Int'l Conf. on Knowledge Discovery and Data mining. New York: ACM, 2003. 206–215. [doi: 10.1145/ 956750.956776]

[62] Gheid Z, Challal Y. Efficient and privacy-preserving *k*-means clustering for big data mining. In: Proc. of the 2016 IEEE Trustcom/BigDataSE/ISPA. Piscataway: IEEE, 2016. 791–798. [doi: 10.1109/TrustCom.2016.0140]

[63] Wang Z, Liu Y, Ma Z, Liu X, Ma J. LiPSG: Lightweight privacy-preserving *Q*-learning based energy management for the IoT-enable smart grid. IEEE Internet of Things Journal, 2020. [doi: 10.1109/JIOT.2020.2968631]

[64] Zhang QC, Yang LT, Chen ZK. Privacy preserving deep computation model on cloud for big data feature learning. IEEE Trans. on Computers, 2016,65(5):1351–1362. [doi: 10.1109/TC.2015.2470255]

[65] Trieu PL, Aono Y, Hayashi T, Wang LH, Moriai S. Privacy-preserving deep learning via additively homomorphic encryption. IEEE Trans. on Information Forensics and Security, 2018,13(5):1333–1345. [doi: 10.1109/TIFS.2017.2787987]

[66] Hesamifard ETH, Ghasemi M, Et A. Privacy-preserving machine learning in cloud. In: Proc. of the 2017 on Cloud Computing Security Workshop. 2017. 39–43. [doi: 10.1145/3140649.3140655]

[67] Chillotti I, Gama N, Georgieva M, Izabachene M. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. In: Proc. of the the Int'l Conf. on the Theory and Application of Cryptology and Information Security. Berlin, Heidelberg: Springer-Verlag, 2016. 3–33. [doi: 10.1007/978-3-662-53887-6_1]

[68] Courbariaux M, Hubara I, Soudry D, El-Yaniv R, Bengio Y. Binarized neural networks: Training deep neural networks with weights and activations constrained to+ 1 or−1. arXiv Preprint arXiv:160202830, 2016.

[69] Kim M, Smaragdis P. Bitwise neural networks. arXiv Preprint arXiv:160106071, 2016.

[70] Bourse F, Minelli M, Minihold M, Paillier P. Fast homomorphic evaluation of deep discretized neural networks. In: Proc. of the Annual Int'l Cryptology Conf. Berlin, Heidelberg: Springer-Verlag, 2018. 483–512. [doi: 10.1007/978-3-319- 96878-0_17]

[71] Mehnaz S, Bellala G, Bertino E. A secure sum protocol and its application to privacy-preserving multi-party analytics. In: Proc. of the 22nd ACM on Symp. on Access Control Models and Technologies. New York: ACM, 2017. 219–230. [doi: 10.1145/ 3078861.3078869]

[72] Bansal A, Chen TT, Zhong S. Privacy preserving back-propagation neural network learning over arbitrarily partitioned data. Neural Computing and Applications, 2011,20(1):143–150. [doi: 10.1007/s00521-010-0346-z]

[73] Jayaraman B, Wang L, Evans D, Gu Q. Distributed learning without distress: Privacy-preserving empirical risk minimization. In: Advances in Neural Information Processing Systems. 2018. 6343–6354.

[74] Xie LY, Lin KX, Wang S, Wang F, Zhou JY. Differentially private generative adversarial network. arXiv Preprint arXiv: 180206739, 2018. [doi: 10.475/123_4]

[75] Bindschaedler V, Shokri R, Gunter CA. Plausible deniability for privacy-preserving data synthesis. Proc. of the VLDB Endowment, 2017,10(5):481–492. [doi: 10.14778/3055540.3055542]

[76] Abadi M, Chu A, Goodfellow I, Mcmahan HB, Mironov I, Talwar K, Zhang L. Deep learning with differential privacy. In: Proc. of the 2016 ACM SIGSAC Conf. on Computer and Communications Security. New York: ACM, 2016. 308–318. [doi: 10.1145/2976749.2978318]

[77] Liu MH, Jiang HT, Chen J, Badokhon A, Wei XT, Huang MC. A collaborative privacy-preserving deep learning system in distributed mobile environment. In: Proc. of the Int'l Conf. on Computational Science and Computational Intelligence. Piscataway: IEEE, 2017. n192–197. [doi: 10.1109/CSCI.2016.42]

[78] Phan N, Wang Y, Wu XT, Dou DJ. Differential privacy preservation for deep auto-encoders: An application of human behavior prediction. In: Proc. of the 30th AAAI Conf. on Artificial Intelligence. Palo Alto: AAAI Press, 2016. 1309–1316.

[79] Papernot N, Song S, Mironov I, Raghunathan A, Talwar K, Erlingsson Ú. Scalable private learning with PATE. arXiv Preprint arXiv:180208908, 2018.

[80] Li M, Chow SS, Hu S, Yan Y, Du M, Wang Z. Optimizing privacy-preserving outsourced convolutional neural network predictions. arXiv Preprint arXiv:200210944, 2020.

[81] Liu L, Su J, Liu X, Chen R, Huang K, Deng RH, Wang X. Toward highly secure yet efficient KNN classification scheme on outsourced cloud data. IEEE Internet of Things Journal, 2019,6(6):9841–9852. [doi: 10.1109/JIOT.2019.2932444]

[82] Dani V, King V, Movahedi M, Saia J, Zamani M. Secure multi-party computation in large networks. Distributed Computing, 2017,30(3):193–229. [doi: 10.1007/s00446-016-0284-9]

[83] Abbasi S, Cimato S, Damiani E. Toward secure clustered multi-party computation: A privacy-preserving clustering protocol. In: Proc. of the Information and Communication Technology-EurAsia Conf. Berlin, Heidelberg: Springer-Verlag, 2013. 447–452. [doi: 10.1007/978-3-642-36818-9_49]

[84] Bogdanov D, Niitsoo M, Toft T, Willemson J. High-performance secure multi-party computation for data mining applications. Int'l Journal of Information Security, 2012,11(6):403–418. [doi: 10.1007/s10207-012-0177-2]

[85] Asharov G, Lindell Y, Schneider T, Zohner M. More efficient oblivious transfer extensions. Journal of Cryptology, 2017,30(3):805–858. [doi: 10.1007/s00145-016-9236-6]

[86] Mohassel P, Zhang YP. SecureML: A system for scalable privacy-preserving machine learning. In: Proc. of the 38th IEEE Symp. on Security and Privacy. Piscataway: IEEE, 2017. 19–38. [doi: 10.1109/SP.2017.12]

[87] Rouhani BD, Riazi MS, Koushanfar F. Deepsecure: Scalable provably-secure deep learning. In: Proc. of the 55th ACM/ESDA/IEEE Design Automation Conf. Piscataway: IEEE, 2018. 1–6. [doi: 10.1145/3195970.3196023]

[88] Liu J, Juuti M, Lu Y, Asokan N. Oblivious neural network predictions via minionn transformations. In: Proc. of the 2017 ACM SIGSAC Conf. on Computer and Communications Security. New York: ACM, 2017. 619–631. [doi: 10.1145/3133956. 3134056]

[89] Chandran N, Gupta D, Rastogi A, Sharma R, Tripathi S. EzPC: Programmable, efficient, and scalable secure two-party computation. ePrint Report, 1109, 2017.

[90] Riazi MS, Weinert C, Tkachenko O, Songhori EM, Schneider T, Koushanfar F. Chameleon: A hybrid secure computation framework for machine learning applications. In: Proc. of the Asia Conf. on Computer and Communications Security. New York: ACM, 2018. 707–721. [doi: 10.1145/3196494.3196522]

[91] Juvekar C, Vaikuntanathan V, Chandrakasan A. Gazelle: A low latency framework for secure neural network inference. In: Proc. of the 27th USENIX Security Symp. 2018. 1651–1669.

[92] Henecka W, Sadeghi A-R, Schneider T, Wehrenberg I. TASTY: Tool for automating secure two-party computations. In: Proc. of the 17th ACM Conf. on Computer and Communications Security. New York: ACM, 2010. 451–462. [doi: 10.1145/1866307.1866358]

[93] Ma Z, Liu Y, Liu X, Ma J, Ren K. Lightweight privacy-preserving ensemble classification for face recognition. IEEE Internet of Things Journal, 2019,6(3):5778–5790. [doi: 10.1109/JIOT.2019.2905555]

[94] Dwork C. Differential privacy. In: Encyclopedia of Cryptography and Security. 2011. 338–340. [doi: 10.1007/11787006_1]

[95] Dwork C, Roth A. The algorithmic foundations of differential privacy. Foundations and Trends® in Theoretical Computer Science, 2014,9(3-4):211–407. [doi: 10.1561/0400000042]

[96] Andrew G, Chien S, Papernot N. TensorFlow privacy. https://github.com/tensorflow/privacy

[97] Kifer D, Lin BR. Towards an axiomatization of statistical privacy and utility. In: Proc. of the 29th ACM SIGMOD-SIGACT-SIGART Symp. on Principles of Database Systems. New York: ACM, 2010. 147–158. [doi: 10.1145/1807085. 1807106]

[98] Dwork C, Rothblum GN, Vadhan S. Boosting and differential privacy. In: Proc. of the 51st IEEE Annual Symp. on Foundations of Computer Science. Piscataway: IEEE, 2010. 51–60. [doi: 10.1109/focs.2010.12]

[99] Ye QQ, Meng XF, Zhu MJ, Huo Z. Survey on local differential privacy. Ruan Jian Xue Bao/Journal of Software, 2018,29(7): 1981–2005 (in Chinese with English abstract). http.//www.jos.org.cn/1000-9825/5364.htm. [doi: 10.13328/j.cnki.jos.005364]

[100] Bindschaedler V, Shokri R. Synthesizing plausible privacy-preserving location traces. In: Proc. of the 2016 IEEE Symp. on Security and Privacy (SP). Piscataway: IEEE, 2016. 546–563. [doi: 10.1109/SP.2016.39]

[101] Bach S, Binder A, Montavon G, Klauschen F, Müller K-R, Samek W. On pixel-wise explanations for non-linear classifier decisions by layer-wise relevance propagation. PloS One, 2015,10(7):e0130140. [doi: 10.1371/journal.pone.0130140]

[102] Chaudhuri K, Monteleoni C, Sarwate AD. Differentially private empirical risk minimization. Journal of Machine Learning Research, 2011,12(Mar.):1069–1109. [doi: 10.1109/MIS.2011.2]

[103] Dwork C, Mcsherry F, Nissim K, Smith A. Calibrating noise to sensitivity in private data analysis. In: Proc. of the Theory of Cryptography Conf. Berlin, Heidelberg: Springer-Verlag, 2006. 265–284. [doi: 10.1007/11681878_14]

[104] Mironov I. Rényi differential privacy. In: Proc. of the 30th IEEE Computer Security Foundations Symp. (CSF). Piscataway: IEEE, 2017. 263–275. [doi: 10.1109/CSF.2017.11]

[105] Wu X, Li F, Kumar A, Chaudhuri K, Jha S, Naughton J. Bolt-on differential privacy for scalable stochastic gradient descent-based analytics. In: Proc. of the 2017 ACM Int'l Conf. on Management of Data. 2017. 1307–1322. [doi: 10.1145/3035918.3064047]

[106] Jayaraman B, Evans D. Evaluating differentially private machine learning in practice. arXiv Preprint arXiv:190208874, 2019.

[107] Graepel T, Lauter K, Naehrig M. ML confidential: Machine learning on encrypted data. In: Proc. of the Int'l Conf. on Information Security and Cryptology. Berlin, Heidelberg: Springer-Verlag, 2012. 1–21. [doi: 10.1007/978-3- 642-37682-5_1]

[108] Li ZY, Gui XL, Gu YJ, Li XS, Dai HJ, Zhang XJ. Survey on homomorphic encryption algorithm and its application in the privacy-preserving for cloud computing. Ruan Jian Xue Bao/Journal of Software, 2018,29(7):1827–1851 (in Chinese with English abstract). http://www. jos.org.cn/1000-9825/5354.htm. [doi: 10.13328/j.cnki.jos.005354]

[109] Acar A, Aksu H, Uluagac AS, Conti M. A survey on homomorphic encryption schemes: Theory and implementation. ACM Computing Surveys, 2018,51(4):79. [doi: 10.1145/3214303]

[110] Gentry C. Fully homomorphic encryption using ideal lattices. In: Proc. of the 41st Annual ACM Symp. on Theory of Computing. New York: ACM, 2009. 169−178. [doi: 10.1109/TIFS.2013.2287732]

[111] Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping. ACM Trans. on Computation Theory, 2014,6(3):13. [doi: 10.1145/2090236.2090262]

[112] El-Yahyaoui A, El Kettani MDE-C. An efficient fully homomorphic encryption scheme. IJ Network Security, 2019,21(1):91–99. [doi: 10.6633/IJNS.20190121(1).11]

[113] Ichibane Y, Gahi Y, Guennoun M, Guennoun Z. Fully homomorphic encryption without noise. Int'l Journal of Smart Security Technologies (IJSST), 2019,6(2):33–51. [doi: 10.4018/IJSST.2019070102]

[114] Chillotti I, Gama N, Georgieva M, Izabachène M. TFHE: Fast fully homomorphic encryption over the torus. Journal of Cryptology, 2020,33(1):34–91.

[115] Baryalai M, Jang-Jaccard J, Liu D. Towards privacy-preserving classification in neural networks. In: Proc. of the 14th Annual Conf. on Privacy, Security and Trust (PST). IEEE, 2016. 392–399. [doi: 10.1109/PST.2016.7906962]

[116] Stone MH. The generalized Weierstrass approximation theorem. Mathematics Magazine, 1948,21(5):237–254. [doi: 10.2307/3029750]

[117] Bos JW, Lauter K, Loftus J, Naehrig M. Improved security for a ring-based fully homomorphic encryption scheme. In: Proc. of the IMA Int'l Conf. on Cryptography and Coding. Berlin, Heidelberg: Springer-Verlag, 2013. 45–64. [doi: 10.1007/978-3-642-45239-0_4]

[118] Naehrig M, Lauter K, Vaikuntanathan V. Can homomorphic encryption be practical. In: Proc. of the 3rd ACM Workshop on Cloud Computing Security Workshop. New York: ACM, 2011. 113–124. [doi: 10.1145/2046660.2046682]

[119] Yao AC. Protocols for secure computations. In: Proc. of the 23rd Annual Symp. on Foundations of Computer Science. Piscataway: IEEE, 1982. 160–164. [doi: 10.1109/SFCS.1982.38]

[120] Rabin MO. How to exchange secrets with oblivious transfer. IACR Cryptology ePrint Archive, 2005,2005:187.

[121] Jiang H, Xu QL. Secure multi-party computation in cloud computing. Journal of Computer Research and Development, 2016, 53(10):2152–2162 (in Chinese with English abstract). [doi: 10.7544/issn1000-1239.2016.20160685]

[122] Ishai Y, Kilian J, Nissim K, Petrank E. Extending oblivious transfers efficiently. In: Proc. of the Annual Int'l Cryptology Conf. Berlin, Heidelberg: Springer-Verlag, 2003. 145–161. [doi: 10.1007/978-3-540-45146-4_9]

[123] Yao AC. How to generate and exchange secrets. In: Proc. of the 27th Annual Symp. on Foundations of Computer Science. Piscataway: IEEE, 1986. 162–167. [doi: 10.1109/SFCS.1986.25]

[124] Lindell Y, Pinkas B. A proof of security of Yao's protocol for two-party computation. Journal of Cryptology, 2009,22(2):161–188. [doi: 10.1007/s00145-008-9036-8]

[125] Bellare M, Hoang VT, Rogaway P. Foundations of garbled circuits. In: Proc. of the 2012 ACM Conf. on Computer and Communications Security. New York: ACM, 2012. 784–796. [doi: 10.1145/2382196.2382279]

[126] Shamir A. How to share a secret. Communications of the ACM, 1979,22(11):612–613. [doi: 10.1007/978-3-642-15328-0_17]

[127] Goldreich O, Micali S, Wigderson A. How to play any mental game. In: Proc. of the 19th Annual ACM Symp. on Theory of Computing. New York: ACM, 1987. 218–229. [doi: 10.1145/28395.28420]

[128] Huang Y. Practical secure two-party computation [Ph.D. Thesis]. Charlottesville: University of Virginia, 2012.

[129] Gascón A, Schoppmann P, Balle B, Raykova M, Doerner J, Zahur S, Evans D. Privacy-preserving distributed linear regression on high-dimensional data. Proc. on Privacy Enhancing Technologies, 2017,2017(4):345–364. [doi: 10.1515/popets-2017-0053]

附中文参考文献:

[28] 周水庚,李丰,陶宇飞,肖小奎.面向数据库应用的隐私保护研究综述.计算机学报,2009,32(5):847–858. [doi: 10.3724/SP.J.1016.2009.00847]

[99] 叶青青,孟小峰,朱敏杰,霍峥.本地化差分隐私研究综述.软件学报,2018,29(7):1981–2005. http.//www.jos.org.cn/1000-9825/5364.htm [doi: 10.13328/j.cnki.jos.005364]

[108] 李宗育,桂小林,顾迎捷,李雪松,戴慧珺,张学军.同态加密技术及其在云计算隐私保护中的应用.软件学报,2018,29(7):1830–1851. http://www.jos.org.cn/1000-9825/5354.htm [doi: 10.13328/j.cnki.jos.005354]

[121] 蒋瀚,徐秋亮.基于云计算服务的安全多方计算.计算机研究与发展,2016,53(10):2152–2162. [doi: 10.7544/issn1000-1239.2016.20160685]

谭作文(1967－),男,博士,教授,博士生导师,主要研究领域为密码学,机器学习隐私保护.

张连福(1978－),男,博士生,主要研究领域为密码学,机器学习隐私保护.