$$D_{sk}(E_{pk_i}(m_1 \circ m_2)) = D_{sk}(E_{pk_i}(m_1) \circ E_{pk_i}(m_2)) \quad (27)$$

$$D_{sk}(E_{pk}(m_1 \circ m_2)) = D_{sk}(E_{pk_i}(m_1) \circ E_{pk_j}(m_2)) \quad (28)$$

$\circ$为密文运算符号,式(21)~式(23)表示不同用户仅能够使用各自的一对公钥私钥对进行加解密,式(24)体现了“多对一”加密方式的特性,不同的用户用各自私钥加密数据发送给同一数据接收者 S 后,S 能够使用自有私钥 sk 进行解密,式(25)、式(26)表示 $P_i(i=1,\ldots,n)$、S 在密钥对(pk_i,sk_i),(pk,sk)下各自支持关于$\circ$的同态运算,式(27)表示 P_i 与 S 在密钥对(pk_i,sk)下支持关于$\circ$的同态运算,式(28)表示 P_i、P_j、S 在$(PK(pk_i,pk_j),sk)$下支持关于$\circ$的同态运算.

References:

[1] Goldreich O, Kushilevitz E, Sudan M. Private information retrieval. Journal of the ACM, 1998,45(6):965–981.

[2] Dan B, Kushilevitz E, Ostrovsky R, *et al*. Public key encryption that allows PIR queries. In: Advances in Cryptology CRYPTO 2007. 2007. 50–67.

[3] Avni H, Dolev S, Gilboa N, *et al*. SSSDB: Database with private information search. In: Algorithmic Aspects of Cloud Computing. Springer Int’l Publishing, 2016.

[4] Song DX, Wagner D, Perrig A. Practical techniques for searches on encrypted data. In: Proc. of the IEEE Symp. on Security and Privacy. 2000. 44–55.

[5] Benaloh J, Chase M, Horvitz E, *et al*. Patient controlled encryption: Ensuring privacy of electronic medical records. In: Proc. of the ACM Cloud Computing Security Workshop, CCSW 2009. Chicago, 2009. 103–114.

[6] Liu Q, Wang G, Wu J. Secure and privacy preserving keyword searching for cloud storage services. Journal of Network & Computer Applications, 2012,35(3):927–933.

[7] Pasupuleti SK, Ramalingam S, Buyya R. An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing. Journal of Network & Computer Applications, 2016,64(C):12–22.

[8] Gajek S. Dynamic symmetric searchable encryption from constrained functional encryption. In: Proc. of the Cryptographers’ Track at the RSA Conf. Cham: Springer-Verlag, 2016. 75–89.

[9] Lindell Y, Pinkas B. Secure multiparty computation for privacy-preserving data mining. Journal of Privacy & Confidentiality, 2012,25(2):761–766.

[10] Damgard I, Polychroniadou A, Rao V. Adaptively secure multi-party computation from LWE (via equivocal FHE). In: Proc. of the Public-Key Cryptography—PKC 2016. Berlin, Heidelberg: Springer-Verlag, 2016.

[11] Huang WR, Gui XL, Yu S, Zhuang W. Privacy-Preserving computable encryption scheme of cloud computing. Chinese Journal of Computers, 2011,(12):2391–2402 (in Chinese with English abstract).

[12] Gentry C. A fully homomorphic encryption scheme [Ph.D. Thesis]. Stanford University, 2009.

[13] Regev O. On lattices, learning with errors, random linear codes, and cryptography. Journal of the ACM, 2009,56(6):1–40.

[14] Stehlé D, Steinfeld R. Making NTRU as secure as worst-case problems over ideal lattices. In: Proc. of the Int’l Conf. on Theory and Applications of Cryptographic Techniques: Advances in Cryptology. Springer-Verlag, 2011. 27–47.

[15] Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) Fully homomorphic encryption without bootstrapping. In: Proc. of the Innovations in Theoretical Computer Science Conf. ACM, 2012. 309–325.

[16] Gentry C, Halevi S. Fully homomorphic encryption without squashing using depth-3 arithmetic circuits. In: Proc. of the 52nd IEEE Annual Symp. on Foundations of Computer Science, FOCS 2011. Palm Springs: IEEE, 2011. 107–116.

[17] Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978,26(2):96–99.

[18] Rivest RL, Adleman L, Dertouzos ML. On data banks and privacy homomorphisms. In: Foundations of Secure Computation. 1978. 169–179.

[19] Elgamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. In: Advances in Cryptology. Berlin, Heidelberg: Springer-Verlag, 1984. 469–472.

[20] Chen L, Xu Y, Fang W, *et al*. A new ElGamal-based algebraic homomorphism and its applications. In: Proc. of the ISECS Int'l Colloquium on Computing, Communication, Control, and Management, CCCM 2008. Guangzhou: IEEE, 2008. 643–648.

[21] Goldwasser S, Micali S. Probabilistic encryption. Journal of Computer Security, 1984,28(2):270–299.

[22] Paillier P. Public-Key cryptosystems based on composite degree residuosity classes. In: Proc. of the Int'l Conf. on Theory and Application of Cryptographic Techniques. Springer-Verlag, 1999. 223–238.

[23] Benaloh J. Verifiable secret-ballot elections [Ph.D. Thesis]. Yale University, 1987.

[24] Okamoto T, Uchiyama S. A new public-key cryptosystem as secure as factoring. In: Proc. of the Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer-Verlag, 1998. 308–318.

[25] Boneh D, Goh EJ, Nissim K. Evaluating 2-DNF formulas on ciphertexts. In: Theory of Cryptography. Berlin: Springer-Verlag, 2005. 325–341.

[26] Dhakar RS, Gupta AK, Sharma P. ModifiedRSA encryption algorithm (MREA). In: Proc. of the 2nd Int'l Conf. on Advanced Computing & Communication Technologies. IEEE, 2012. 426–429.

[27] Stehlé D, Steinfeld R. Faster fully homomorphic encryption. In: Advances in Cryptology-ASIACRYPT 2010, Proc. of the Int'l Conf. on the Theory and Application of Cryptology and Information Security. Singapore, 2010. 377–394.

[28] Bos JW, Lauter K, Naehrig M. Private predictive analysis on encrypted medical data. Journal of Biomedical Informatics, 2014, 50(8):234–243.

[29] Lauter K, López-Alt A, Naehrig M. Private computation on encrypted genomic data. In: Progress in Cryptology-LATINCRYPT 2014. Springer Int'l Publishing, 2014. 3–27.

[30] Dowlin N, Ran GB, Laine K, *et al*. Manual for using homomorphic encryption for bioinformatics. Proc. of the IEEE, 2017,105(3): 552–567.

[31] Miran K, Kristin L. Private genome analysis through homomorphic encryption. BMC Medical Informatics & Decision Making, 2015,15(S5):1–12.

[32] Castelluccia C, Mykletun E, Mykletun E, *et al*. Efficient and provably secure aggregation of encrypted data in wireless sensor networks. ACM Trans. on Sensor Networks, 2009,5(3):20.

[33] Boneh D, Gentry C, Halevi S, Wang F, Wu DJ. Private database queries using somewhat homomorphic encryption. In: Proc. of the ACNS 2013: Applied Cryptography and Network Security. 2013. 102–118.

[34] Hall R, Fienberg S, Nardi Y. Secure multiple linear regression based on homomorphic encryption. Official Statistics, 2011,27(4): 669–691.

[35] Yasuda M, Shimoyama T, Kogure J, *et al*. Secure statistical analysis using RLWE-based homomorphic encryption. Lecture Notes in Computer Science, 2015,9144:471–487.

[36] Gentry C, Halevi S, Vaikuntanathan V. A simple BGN-type cryptosystem from LWE. In: Proc. of the Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer-Verlag, 2010. 506–522.

[37] Chan CF. Symmetric-Key homomorphic encryption for encrypted data processing. In: Proc. of the IEEE Int'l Conf. on Communications. IEEE, 2009. 1–5.

[38] Hojsík M, Plapanova V. A fully homomorphic cryptosystem with approximate perfect secrecy. In: Dawson E, ed. Topics in Cryptology—CT-RSA 2013. Berlin, Heidelberg: Springer-Verlag, 2013. 375–388.

[39] Yang P, Gui XL, Yu J, Lin JC, Tian F, Zhang XJ. Research on algorithms of data encryption scheme that supports homomorphic arithmetical operations. Journal on Communications, 2015,36(1):171–182 (in Chinese with English abstract).

[40] Smart NP, Vercauteren F. Fully homomorphic encryption with relatively small key and ciphertext sizes. In: Proc. of the Int'l Conf. on Practice and Theory in Public Key Cryptography. Springer-Verlag, 2010. 420–443.

[41] Chen, ZG, Wang J, Zhang ZN, *et al*. A fully homomorphic encryption scheme with better key size. China Communications, 2014,11(9):82–92.

[42] Gentry C, Halevi S, Smart N. Better bootstrapping in fully homomorphic encryption. In: Fischlin M, Buchmann J, Manulis M, eds. Public Key Cryptography–PKC 2012. Berlin, Heidelberg: Springer-Verlag, 2012. 1–16.

[43] Gentry C, Halev Si. Implementing Gentry's fully-homomorphic encryption scheme. In: Proc. of the Int'l Conf. on Theory and Applications of Cryptographic Techniques: Advances in Cryptology. Springer-Verlag, 2014. 129–148.

[44] Dijk MV, Gentry C, Halevi S, *et al*. Fully homomorphic encryption over the integers. In: Proc. of the Int'l Conf. on Theory and Applications of Cryptographic Techniques. Springer-Verlag, 2010. 24–43.

[45] Bogdanov A, Lee CH. Homomorphic encryption from codes. Eprint Arxiv, 2011.

[46] Chillotti I, Gama N, Georgieva M, *et al*. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. In: Advances in Cryptology—ASIACRYPT 2016. Berlin, Heidelberg: Springer-Verlag, 2016.

[47] Yagisawa M. Fully homomorphic encryption without bootstrapping. ACM Trans. on Computation Theory, 2015,6(3):1–36.

[48] Chan CF. Symmetric-Key homomorphic encryption for encrypted data processing. In: Proc. of the IEEE Int'l Conf. on Communications. IEEE, 2009. 1–5.

[49] Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) fully homomorphic encryption without bootstrapping. In: Proc. of the 3rd Innovations in Theoretical Computer Science Conf., ITCS 2012. Cambridge: ACM, 2012. 309–325.

[50] Brakerski Z, Vaikuntanathan V. Fully homomorphic encryption from ring-LWE and security for key dependent messages. In: Proc. of the Cryptology Conf. Berlin, Heidelberg: Springer-Verlag, 2011. 505–524.

[51] Gu C. More practical fully homomorphic encryption. Int'l Journal of Cloud Computing and Services Science, 2012, 1–17.

[52] Kipnis A, Hibshoosh E. Efficient methods for practical fully homomorphic symmetric-key encrypton, randomization and verification. Uiban Research & Practice, 2012,7(3):255–257.

[53] Gentry C, Halevi S, Smart NP. Homomorphic evaluation of the AES circuit. In: Advances in Cryptology–CRYPTO 2012. Berlin, Heidelberg: Springer-Verlag, 2012. 850–867.

[54] Gentry C, Halevi S, Smart N. Fully homomorphic encryption with polylog overhead. In: Advanced in Cryptology–EUROCRYPT. LNCS 7237, 2012. 465–482.

[55] Tromer E, Vaikuntanathan V. On-the-Fly multiparty computation on the cloud via multikey fully homomorphic encryption. In: Proc. of the 44th ACM Symp. on Theory of Computing. ACM, 2012. 1219–1234.

[56] Brakerski Z. Fully homomorphic encryption without modulus switching from classical GapSVP. In: Advances in Cryptology –CRYPTO 2012. Berlin, Heidelberg: Springer-Verlag, 2012. 868–886.

[57] Naccache D, Tibouchi M. Public key compression and modulus switching for fully homomorphic encryption over the integers. In: Proc. of the Int'l Conf. on Theory and Applications of Cryptographic Techniques. Springer-Verlag, 2012. 446–464.

[58] Zhang W, Liu S, Yang X. RLWE-Based homomorphic encryption and private information retrieval. In: Proc. of the Int'l Conf. on Intelligent NETWORKING and Collaborative Systems. IEEE, 2013. 535–540.

[59] Bos JW, Lauter K, Loftus J, *et al*. Improved security for a ring-based fully homomorphic encryption scheme. In: Cryptography and Coding. Berlin, Heidelberg: Springer-Verlag, 2013. 45–64.

[60] Cheon JH, Kim J, Lee MS, *et al*. CRT-Based fully homomorphic encryption over the integers. Information Sciences, 2015, 310(C):149–162.

[61] Zhang L, Yue Q. A fast integer-based batch full-homomorphic encryption scheme over finite field. IACR Cryptology ePrint Archive, 2013.

[62] Cheon JH, Coron JS, Kim J, *et al*. Batch fully homomorphic encryption over the integers. In: Proc. of the Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer-Verlag, 2013. 315–335.

[63] Pisa PS, Abdalla M, Duarte OCMB. Somewhat homomorphic encryption scheme for arithmetic operations on large integers. In: Proc. of the Global Information Infrastructure & Networking Symp. IEEE, 2013. 1–8.

[64] Doroz Y, Hu Y, Sunar B. Homomorphic AES evaluation using NTRU. IACR Cryptology ePrint Archive, 2014. 1–16.

[65] Doröz Y, Shahverdi A, Eisenbarth T, *et al*. Toward practical homomorphic evaluation of block ciphers using prince. In: Proc. of the Int'l Conf. on Financial Cryptography and Data Security. Berlin, Heidelberg: Springer-Verlag, 2014. 208–220.

[66] Chen Z, Wang J, Song X. A regev-type fully homomorphic encryption scheme using modulus switching. The Scientific World Journal, 2014,17(21):331–342.

[67] Coron J, Lepoint T, Tibouchi M. Scale-Invariant fully homomorphic encryption over the integers. LLAR Journal, 2014,50(4): 361–372.

[68] Zhou H, Wornell G. Efficient homomorphic encryption on integer vectors and its applications. In: Proc. of the Information Theory and Applications Workshop. 2014. 1–9.

[69] Rohloff K, Cousins DB. A scalable implementation of fully homomorphic encryption built on NTRU. In: Proc. of the WAHC 2014 Workshop on Applied Homomorphic Cryptography and Encrypted Computing. 2014. 221–234.

[70] Wang C, Ren K, Wang J. Secure optimization computation outsourcing in cloud computing: A case study of linear programming. IEEE Trans. on Computers, 2016,65(1):216–229.

[71] Chen X, Huang X, Li J, *et al*. New algorithms for secure outsourcing of large-scale systems of linear equations. IEEE Trans. on Information Forensics and Security, 2015,10(1):69–78.

[72] Alderman J, Janson C, Cid C, *et al*. Hybrid publicly verifiable computation. In: Topics in Cryptology-CT-RSA 2016. Springer Int'l Publishing, 2016.

[73] Hu Y. Improving the efficiency of homomorphic encryption schemes [Ph.D. Thesis]. Worcester: Department of Electrical and Computer Engineering, Worcester Polytechnic Institute, 2013.

[74] Clear M, Mcgoldrick C. Bootstrappable identity-based fully homomorphic encryption. In: Proc. of the Cryptology and Network Security. Springer Int'l Publishing, 2014. 1–19.

[75] Coron JS, Mandal A, Naccache D, *et al*. Fully homomorphic encryption over the integers with shorter public keys. In: Rogaway P, ed. Advances in Cryptology–CRYPTO 2011. Berlin, Heidelberg: Springer-Verlag, 2011. 487–504.

[76] Lepoint T, Naehrig M. A comparison of the homomorphic encryption schemes FV and YASHE. In: Proc. of the Int'l Conf. on Cryptology in Africa. Springer Int'l Publishing, 2014. 318–335.

[77] Smart NP, Vercauteren F. Fully homomorphic SIMD operations. Designs Codes & Cryptography, 2014,71(1):57–81.

[78] Gopal GN, Singh MP. Secure similarity based document retrieval system incloud. In: Proc. of the 2012 Int'l Conf. on Data Science Engineering (ICDSE). 2012. 154–159.

[79] Wang CN, Li C, Ren M, Lou WK. Privacy-Preserving multi-keyword ranked search over encrypted cloud data. IEEE Trans. on Parallel and Distributed Systems, 2014,25(1):222–233.

[80] Li J, Wang Q, Wang C, *et al*. Fuzzy keyword search over encrypted data in cloud computing. In: Proc. of the Conf. on Information Communications. IEEE Press, 2010. 441–445.

[81] Bendlin R, Damgard I, Orlandi C, *et al*. Semi-Homomorphic encryption and multiparty computation. Lecture Notes in Computer Science, 2011,6632(2010):169–188.

[82] Lin HY, Tzeng WG. An efficient solution to the millionaires' problem based on homomorphic encryption. In: Proc. of the Int'l Conf. on Applied Cryptography and Network Security. Springer-Verlag, 2005. 456–466.

[83] Goethals B, Laur S, Lipmaa H, *et al*. On private scalar product computation for privacy-preserving data mining. In: Proc. of the Int'l Conf. on Information Security and Cryptology. Springer-Verlag, 2004. 104–120.

[84] Tu S, Kaashoek M, Madden S, Zeldovich N. Processing analytical queries over encrypted data. Int'l Conf. on Very Large Data Bases, 2013,6(5):289–300.

[85] Tetali SD, Lesani M, Majumdar R, *et al*. MrCrypt: Static analysis for secure cloud computations. In: Proc. of the ACM Sigplan Int'l Conf. on Object Oriented Programming Systems Languages & Applications. ACM, 2013. 271–286.

[86] Stephen JJ, Savvides S, Seidel R, *et al*. Practical confidentiality preserving big data analysis. In: Proc. of the Usenix Conf. on Hot Topics in Cloud Computing. USENIX Association, 2014. 10.

[87] Brenner M, Wiebelitz J, Voigt GV, *et al*. Secret program execution in the cloud applying homomorphic encryption. In: Proc. of the IEEE Int'l Conf. on Digital Ecosystems and Technologies. IEEE, 2011. 114–119.

[88] Lu CS. Homomorphic encryption-based secure SIFT for privacy-preserving feature extraction. In: Proc. of the SPIE-The Int'l Society for Optical Engineering, 2011,7880(2):788005-788005-17.

[89] Ren W, Ren Y, Zhang H. H2S: A secure and efficient data aggregative retrieval scheme in unattended wireless sensor networks. In: Proc. of the 5th Int'l Conf. on Information Assurance and Security. IEEE Computer Society, 2009. 450–453.

[90] Zhu H, Bao F. Private searching on MapReduce. In: Proc. of the Int'l Conf. on Trust, Privacy and Security in Digital Business, Trustbus 2010. Bilbao, 2010. 93–101.

[91] Zhu HH, He QH, Zhu HH, *et al*. Voiceprint-Biometric template design and authentication based on cloud computing security. In: Proc. of the Int'l Conf. on Cloud and Service Computing. IEEE Computer Society, 2011. 302–308.

[92] Bilogrevic I, Jadliwala M, Kumar P, *et al*. Meetings through the cloud: Privacy-Preserving scheduling on mobile devices. Journal of Systems & Software, 2011,84(11):1910–1927.

[93] Liu Y, Ren W. Robust and secure yet simple data collection in WSNs applying to marine gas turbine. In: Proc. of the Int'l Conf. on Multimedia Information NETWORKING and Security. IEEE Computer Society, 2009. 360–364.

[94] Upmanyu M, Namboodiri AM, Srinathan K, *et al*. Efficient privacy preserving *K*-means clustering. In: Intelligence and Security Informatics. Berlin, Heidelberg: Springer-Verlag, 2010. 154–166.

[95] Ren Y, Oleshchuk V, Li FY. Secure and efficient data storage in unattended wireless sensor networks. In: Proc. of the Int'l Conf. on New Technologies, Mobility and Security. IEEE Press, 2009. 244–248.

[96] Lipmaa H, Zhang B. Two new efficient PIR-writing protocols. Lecture Notes in Computer Science, 2010,6123:438–455.

[97] Ma J, Li F, Li JH. Perturbation method for distributed privacy-preserving data mining. Journal of Zhejiang University, 2010, 44(2):276–282 (in Chinese with English abstract).

[98] Fang WW, Hu J, Yang BR, Zhou CS. Research of privacy-preserving in distributed decision-tree mining. Coputer Science, 2009,36(4):239–242 (in Chinese with English abstract).

[99] Jaideep V, Murat K, Chris C. Privacy-Preserving Naïve Bayes classification. The VLDB Journal, 2008,17:879–898.

[100] Vaidya J, Yu H, Jiang X. Privacy-Preserving SVM classification. Knowledge & Information Systems, 2008,14(2):161–178.

[101] Nuida K. Candidate constructions of fully homomorphic encryption on finite simple groups without ciphertext noise. Technical Report, 2014/97, 2015.

[102] Yagisawa M. Fully homomorphic public-key encryption based on discrete logarithm problem. Technical Report, 2016/054, 2016.

[103] Downlin N, Bachrach RG, Laine K, Lauter K, Naehrig M, Wernsing J. CryptoNets: Applying neural networks to encrypted data with high throughput and accuracy. Microsoft Research Technical Report, MSR-TR-2016-3, 2016.

附中文参考文献:

[11] 黄汝维,桂小林,余思,庄威.云环境中支持隐私保护的可计算加密方法.计算机学报,2011,(12):2391–2402.

[39] 杨攀,桂小林,姚婧,林建财,田丰,张学军.支持同态算术运算的数据加密方法算法研究.通信学报,2015,36(1):171–182.

[97] 马进,李锋,李建华.分布式数据挖掘中基于扰乱的隐私保护方法.浙江大学学报,2010,44(2):276–282.

[98] 方炜炜,胡健,杨炳儒,周长胜.分布式决策树挖掘的隐私保护研究.计算机科学,2009,36(4):239–242.

李宗育(1985－),男,江西上饶人,博士生,CCF 学生会员,主要研究领域为云计算隐私保护,密码学.

李雪松(1992－),男,硕士,CCF 学生会员,主要研究领域为密码学,区块链.

桂小林(1966－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为云计算隐私保护,网络安全,可信计算.

戴慧珺(1979－),女,博士,工程师,CCF 专业会员,主要研究领域为隐私保护,加密计算.

顾迎捷(1992－),男,博士生,主要研究领域为信息安全,区块链技术.

张学军(1977－),男,博士,副教授,CCF 专业会员,主要研究领域为位置隐私保护与度量,云安全.