他方案都快,仅需要 1s 左右.

图 8 反映了解密时间的变化情况.单授权方案与本方案因为均需遍历所有的访问控制结构,因此在属性数目较小的情况下(0~40),Chase、Li 方案的计算时间更快,但是随着属性的增加,多属性中心在解密速度上更快,反映了一定的适应性.

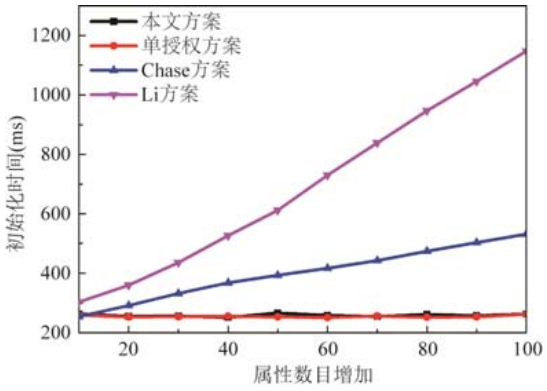

Fig.5 System initialization time (attribute change)

图 5 属性数目递增系统初始化时间图

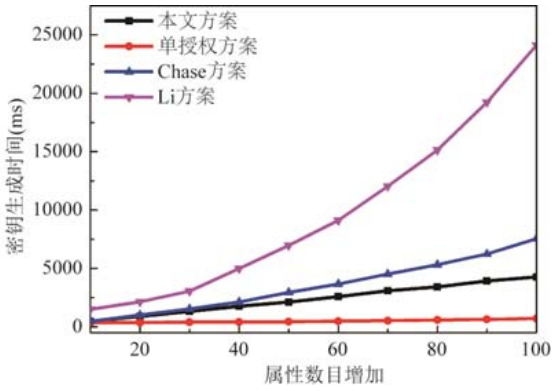

Fig.6 System key generation time (attribute change)

图 6 属性数目递增密钥生成时间图

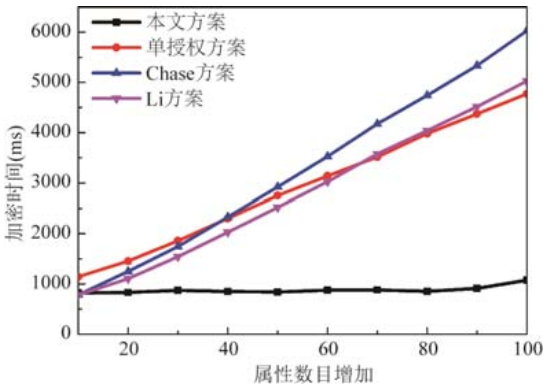

Fig.7 System encryption time (attribute change)

图 7 属性数目递增加密时间图

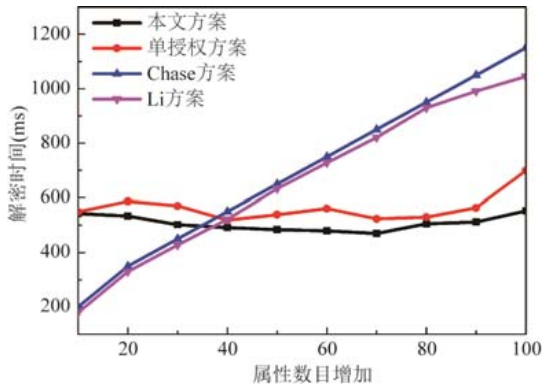

Fig.8 System decryption time (attribute change)

图 8 属性数目递增解密时间图

同时,因为上文中 Chase、Li 方案的计算效率与多授权以及单授权方案相比,差距较大,为了进一步区分与单授权中心计算的差异性并验证第 6.2 节计算开销和通信开销分析的正确性,本文扩展了属性数目固定为 50 个,访问控制策略为 3 层,数据文件大小从 10M~100M 逐渐递增的实验,进行了补充对比.

图 9 说明,在同样属性数目和访问控制策略下,随着文件大小的递增,系统初始化时间基本稳定,与单授权方案持平.

图 10 说明单授权中心在产生密钥的速度上具有优势,这是因为,多授权中心为了解决单授权中心密钥托管的风险问题,子密钥由多个属性中心分别计算,因此时间开销较大.但是多授权中心在加密时间上体现了较大的优越性,如图 11 所示,虽然两者在密钥生成时间上相差 30ms 左右,但在加密时间上却快了 1 000 多 ms,因此,非常适合应用在移动终端的工作环境.

图 12 反映了解密时间的变化情况,解密 100M 的文件在 1.4s 之内,依然有很快的速度,不会影响到用户的实际体验.总的看来,本方案在系统初始化、密钥生成、属性加密和解密的总时间上优于单授权中心方案.

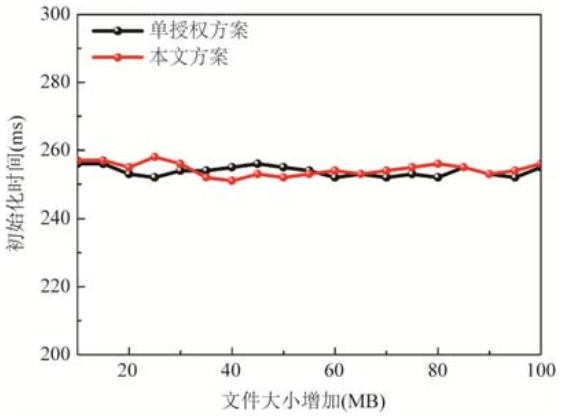

Fig.9 System initialization time (file change)

图 9 文件大小递增初始化时间图

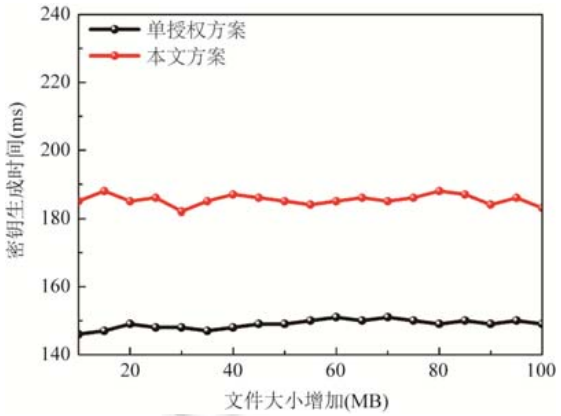

Fig.10 System key generation time (file change)

图 10 文件大小递增密钥生成时间图

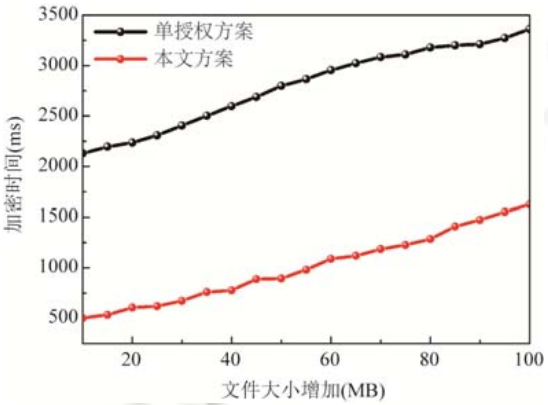

Fig.11 System encryption time (file change)

图 11 文件大小递增加密时间图

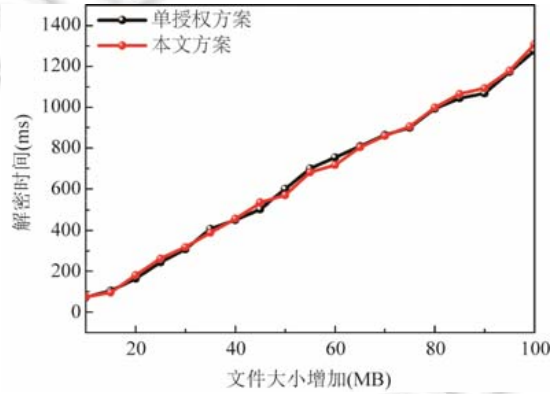

Fig.12 System decryption time (file change)

图 12 文件大小递增解密时间图

最后,我们与其他方案进行了适应性比较.通过比较发现,在我们的方案中,循环群计算次数只应用了一次 p 运算,在访问控制结构上适应多属性的门限方案(AND-gates +/–支持多属性)、通配符计算以及可以隐藏访问控制结构(hidden policy),体现了更好的适应性.见表 4.

Table 4 Comparions among CP-ABE schemes

表 4 与其他 CP-ABE 方案的适应性比较

方案	循环群计算次数	门限方案	通配符	隐藏访问控制策略
Lai, *et al*.[30]	*pqr*	AND-gates +/– on	√	×
Chen, *et al*.[31]	*pqr*	Threshold gates	×	×
Li, *et al*.[32]	*pq*	AND-gates +/– on multi-valued attributes	×	√
本方案	*p*	AND-gates +/– on multi-valued attributes	√	√

7 结束语

在移动社交网络中,用户之间最大化地增强彼此之间的联系和交流,同时又要保护用户的个人隐私问题是当前隐私保护方向的一个研究热点.本文基于密码学的研究,提出了多授权中心基于属性的加密方案,该方案提高了移动社交网络中的交友效率,解决了以往单一授权中心的性能瓶颈和密钥管理问题,使得用户能够细粒度地发现与自身设定访问控制策略相匹配的用户,同时可以保证用户交友过程中的隐私不被泄漏.

References:

[1] Fu YY, Zhang M, Feng DG, Chen KQ. Attribute privacy preservation in social networks based on node anatomy. Ruan Jian Xue Bao/Journal of Software, 2014,25(4):768−780 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4565.htm [doi: 10.13328/j.cnki.jos.004565]

[2] Zhang L, Li XY, Liu Y. Message in a sealed bottle: Privacy preserving friending in social networks. IEEE Trans. on Mobile Computing, 2015,14(9):1888−1902. [doi: 10.1109/TMC.2014.2366773]

[3] Wang Y, Vasilakos AV, Jin Q. Survey on mobile social networking in proximity (MSNP): Approaches, challenges and architecture. Wireless Networks, 2013,20(6):1295−1311. [doi :10.1007/s11276-013-0677-7]

[4] Guo L, Zhang C, Sun J. A privacy-preserving attribute-based authentication system for mobile health networks. IEEE Trans. on Mobile Computing, 2014,13(9):1927−1941. [doi: 10.1109/TMC.2013.84]

[5] Guo L, Zhu X, Zhang C. Privacy-Preserving attribute-based friend search in geosocial networks with untrusted servers. In: Proc. of the Int'l Conf. Global Communications Conf. 2013. 629−634. [doi: 10.1109/GLOCOM.2013.6831142]

[6] Lu R, Lin X, Liang X, Shen X. A secure handshake scheme with symptoms-matching for healthcare social network. Mobile Networks and Applications, 2011,16(6):683−694. [doi: 10.1007/s11036-010-0274-2]

[7] Sarpong S, Xu C. A secure and efficient privacy-preserving attribute matchmaking protocol in proximity-based mobile social networks. In: Proc. of the Int'l Conf. Advanced Data Mining and Applications. 2014. 305−318.

[8] Li M, Cao N, Yu S, Lou W. Findu: Privacy-Preserving personal profile matching in mobile social networks. In: Proc. of the Int'l Conf. Computer Communications (INFOCOM). 2011. 2435−2443. [doi: 10.1109/INFCOM.2011.5935065]

[9] Yan Z, Ding W, Niemi V. Two schemes of privacy-preserving trust evaluation. Future Generation Computer Systems, 2015,62(C): 175−189. [doi: 10.1016/j.future.2015.11.006]

[10] Kiraz MS, Genc ZA, Kardas S. Security and efficiency analysis of the Hamming distance computation protocol based on oblivious transfer. Security & Communication Networks, 2015,8(18):4123−4135. [doi: 10.1002/sec.1329]

[11] Ozdemir S, Peng M, Xiao Y. PRDA: Polynomial regression-based privacy-preserving data aggregation for wireless sensor networks. Wireless Communications & Mobile Computing, 2013,15(4):615−628. [doi: 10.1002/wcm.2369]

[12] Zhang R, Zhang J, Zhang Y, Sun J. Privacy-Preserving profile matching for proximity-based mobile social networking. IEEE Journal on Selected Areas in Communications, 2013,31(9):656−668. [doi: 10.1109/JSAC.2013.SUP.0513057]

[13] Niu B, Zhu X, Liu J. Weight-Aware private matching scheme for proximity-based mobile social networks. In: Proc. of the IEEE Global Communications Conf. (GLOBECOM). 2013. 3170−3175. [doi: 10.1109/GLOCOM.2013.6831559]

[14] Zhu X, Chen Z, Chi H. Two-Party and multi-party private matching for proximity-based mobile social networks. In: Proc. of the Int'l Conf. Communications (ICC). 2014. 926−931. [doi: 10.1109/ICC.2014.6883438]

[15] Han J, Susilo W, Mu Y. Privacy-Preserving decentralized key-policy attribute-based encryption. IEEE Trans. on Parallel & Distributed Systems, 2012,23(11):2150−2162. [doi: 10.1109/TPDS.2012.50]

[16] Lewko A, Ostrovsky R, Sahai A, Waters B. Attribute-Based encryption with non-monotonic access structures. In: Proc. of the Int'l Conf. Computer and Communications Security. 2007. 195−203. [doi: 10.1145/1315245.1315270]

[17] Lewko A, Okamoto T, Sahai A, Waters B. Fully secure functional encryption: Attribute-Based encryption and (hierarchical) inner product encryption. In: Proc. of the Int'l Conf. Theory and Applications of Cryptographic Techniques. 2010. 62−91. [doi: 10.1007/978-3-642-13190-5_4]

[18] Lewko A, Okamoto T, Takashima K, Waters B. Fully secure functional encryption with general relations from the decisional linear assumption. In: Proc. of the Int'l Conf.CRYPTO. 2010. 191−208. [doi: 10.1007/978-3-642-14623-7_11]

[19] Waters B. Ciphertext-Policy attribute-based encryption: An expressive, efficient, and provably secure realization. In: Proc. of the Int'l Conf. Practice and Theory in Public Key Cryptography. 2011. 53−70. [doi: 10.1007/978-3-642-19379-8_4]

[20] Bethencourt J, Sahai A, Waters B. Ciphertext-Policy attribute-based encryption. In: Proc. of the Int'l Conf .Symp. on Security and Privacy. 2007. 321−334. [doi: 10.1109/SP.2007.11]

[21] Cheung L, Newport C. Provably secure ciphertext policy ABE. In: Proc. of the Int'l Conf. Computer and Communications Security. 2007. 456−465. [doi: 10.1145/1315245.1315302]

[22] Zhou Z, Huang D, Wang Z. Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption. IEEE Trans. on Computers, 2015,64(1):126–138. [doi: 10.1109/TC.2013.200]

[23] Shamir A. How to share a secret. Communications of the ACM, 1979,22(11):612–613. [doi: 10.1145/359168.359176]

[24] Blakley GR. Safeguarding cryptographic keys. In: Proc. of the Int'l Conf. Computer Society. 1979. 313–317. [doi: 10.1109/AFIPS.1979.98]

[25] Cramer R, Shoup V. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Proc. of the Int'l Conf. Advances in Cryptology—CRYPTO'98. 1998. 13–25. [doi: 10.1007/BFb0055717]

[26] Wei FS, Zhang G, Ma JF, Ma CG. Privacy-Preserving multi-factor key exchange protocol in the standard model. Ruan Jian Xue Bao/Journal of Software, 2016,27(6):1511–1522 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5001.htm [doi: 10.13328/j.cnki.jos.005001]

[27] Luo E, Wang W, Meng D. A privacy preserving friend discovery strategy using proxy re-encryption in mobile social networks. In: Proc. of the Int'l Conf. Security, Privacy, and Anonymity in Computation, Communication, and Storage. 2016. 190–203. [doi: 10.1007/978-3-319-49148-6_17]

[28] Chase M, Chow SSM. Improving privacy and security in multi-authority attribute-based encryption. In: Proc. of the Int'l Conf. Computer and Communications Security. 2009. 121–130. [doi: 10.1145/1653662.1653678]

[29] Li J, Huang Q, Chen X. Multi-Authority ciphertext-policy attribute-based encryption with accountability. In: Proc. of the Int'l Conf. Symp. on Information, Computer and Communications Security. 2011. 386–390. [doi: 10.1145/1966913.1966964]

[30] Lai J, Deng R, Li Y. Fully secure cipertext-policy hiding CP-ABE. In: Proc. of the Int'l Conf. Information Security Practice and Experience. 2011. 24–39. [doi: 10.1007/978-3-642-21031-0_3]

[31] Chen C, Chen J, Lim HW, Zhang Z, Feng D. Fully secure attribute-based systems with short ciphertexts/signatures and threshold access structures. In: Proc. of the Int'l Conf. Cryptographers Track at the RSA. 2013. 50–60. [doi: 10.1007/978-3-642-36095-4_4]

[32] Li X, Gu D, Ren Y, Ding NK. Efficient ciphertextpolicy attribute based encryption with hidden policy. In: Proc. of the Int'l Conf. Internet and Distributed Computing Systems. 2012. 146–159. [doi: 10.1007/978-3-642-34883-9_12]

附中文参考文献:

[1] 付艳艳,张敏,冯登国,陈开渠.基于节点分割的社交网络属性隐私保护.软件学报,2014,25(4):768–780. http://www.jos.org.cn/1000-9825/4565.htm [doi: 10.13328/j.cnki.jos.004565]

[26] 魏福山,张刚,马建峰,马传贵.标准模型下隐私保护的多因素密钥交换协议.软件学报,2016,27(6):1511–1522. http://www.jos.org.cn/1000-9825/5001.htm [doi: 10.13328/j.cnki.jos.005001]

罗恩韬(1978－),男,湖南永州人,博士,副教授,主要研究领域为移动社交网络隐私保护,云安全,大数据聚类分析.

刘琴(1982－),女,博士,助理教授,CCF 专业会员,主要研究领域为云安全,信息安全,隐私保护.

王国军(1970－),男,博士,教授,博士生导师,CCF 杰出会员,主要研究领域为可信计算,净室安全计算,网络空间安全.

孟大程(1994－),男,硕士,主要研究领域为移动医疗网络隐私保护,大数据安全.