Qiang Tang

*

Publications

International Journal

[Journal1]Q. Tang and J. Wang. Privacy-preserving friendship-based recommender systems. *IEEE Transactions on Dependable and Secure Computing (TDSC)*, ??(??):1–13, 2016.

[Journal2]X. Chen, W. Susilo, J. Li, D. S. Wong, J. Ma, S. Tang, and Q. Tang. Efficient algorithms for secure outsourcing of bilinear pairings. *Theoretical Computer Science*, 562:112–121, 2015.

[Journal3]Q. Tang. From ephemerizer to timed-ephemerizer - achieve assured lifecycle enforcement for sensitive data. *The Computer Journal*, pages 1003–1020, 2015.

[Journal4]Q. Tang, H. Ma, and X. Chen. Extend the concept of public key encryption with delegated search. *The Computer Journal*, pages 724–734, 2015.

[Journal5]X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou. New algorithms for secure outsourcing of modular exponentiations (full paper). *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, 25(9):2386–2396, 2014.

[Journal6]Q. Tang. Nothing is for free: Security in searching shared & encrypted data. *IEEE Transactions on Information Forensics & Security (TIFS)*, pages 1943–1952, 2014.

[Journal7]D. Khader, Q. Tang, and P. Ryan. Proving pret a voter receipt free using computational security models. *USENIX Journal of Election Technology and Systems (JETS)*, 1(1):62–81, 2013.

[Journal8]J. Wang, H. Ma, Q. Tang, J. Li, H. Zhu, S. Ma, and X. Chen. Efficient verifiable fuzzy keyword search over encrypted data in cloud computing. *Comput. Sci. Inf. Syst.*, 10(2):667–684, 2013.

[Journal9]Q. Tang. Public key encryption schemes supporting equality test with authorization of different granularity. *International Journal of Applied Cryptography*, 2(4):304–321, 2012.

[Journal10]Q. Tang. Public key encryption supporting plaintext equality test and user-specified authorization. *Security and Communication Networks*, 5(12):1351–1362, 2012.

[Journal11]J. Wang, H. Ma, Q. Tang, J. Li, H. Zhu, S. Ma, and X. Chen. A new efficient verifiable fuzzy keyword search scheme. *JoWUA*, 3(4):61–71, 2012.

[Journal12]Y. Zhao, X. Chen, H. Ma, Q. Tang, and H. Zhu. A new trapdoor-indistinguishable public key encryption with keyword search. *JoWUA*, 3(1/2):72–81, 2012.

[Journal13]Q. Tang and L. Chen. Extended kci attack against two-party key establishment protocols. *Information Processing Letters*, 111(15):744–747, 2011.

[Journal14]Q. Tang and A. Jeckmans. Towards a security model for computational puzzle schemes. *International Journal of Computer Mathematics*, 88(11):2246–2257, 2011.

[Journal15]I. Buhan, J. Doumen, P. Hartel, Q. Tang, and R. Veldhuis. Embedding renewable cryptographic keys into continuous noisy data (full paper). *International Journal of Information Security*, 9(3):193–208, 2010.

[Journal16]L. Ibraimi, Q. Tang, P. Hartel, and W. Jonker. Exploring type-and-identity-based proxy re-encryption scheme to securely manage personal health records. *Special Issue of International Journal of Computational Models and Algorithms in Medicine (IJCMAM)*, 1(2):1–21, 2010.

[Journal17]Q. Tang and L. Chen. Bilateral unknown key-share attacks in key agreement protocols. *Journal of Universal Computer Science*, 14(3):416–440, 2008.

[Journal18]Q. Tang. On the security of a group key agreement protocol. *Computer Journal*, 50(5):589–590, 2007.

[Journal19]Q. Tang and C. J. Mitchell. Cryptanalysis of a hybrid authentication protocol for large mobile networks. *Journal of Systems and Software*, 79(4):496–501, 2006.

[Journal20]Q. Tang and C. J. Mitchell. Comments on a cryptographic key assignment scheme. *Computer Standards & Interfaces*, 27(4):323–326, 2005.

[Journal21]Q. Tang and C. J. Mitchell. Comments on two anonymous key distribution systems. *Computer Standards & Interfaces*, 27(4):397–400, 2005.

[Journal22]Q. Tang and C. J. Mitchell. Cryptanalysis of two identification schemes based on an id-based cryptosystem. *IEE Proceedings Communications*, 152(5):723–724, 2005.

Book Chapter

[Journal23]J. Li, S. A. Sattar, J. Liu M. M. Baig, R. Heatherly, Q. Tang, and B. Malin. *Medical Data Privacy Handbook*, chapter Methods to Mitigate Risk of Composition Attack in Independent Data Publications, pages 179–200. Springer, 2015.

[Journal24]M. Beye, A. Jeckmans, Z. Erkin, Q. Tang, P. Hartel, and I. Lagendijk. *Social Media Retrieval*, chapter Privacy in Recommender systems, pages 263–281. Springer, 2013.

[Journal25]Q. Tang. *Theory and Practice of Cryptography Solutions for Secure Information Systems*, chapter Search in Encrypted Data: Theoretical Models and Practical Applications, pages 84–108. IGI, 2013.

[Journal26]M. Beye, A. Jeckmans, Z. Erkin, Q. Tang, P. Hartel, and I. Lagendijk. *Social Network Book*, chapter Privacy in Online Social Networks, pages 87–113. Springer, 2012.

Conference and Workshop (2016-2018)

[Conference27]A. Arriaga, V. Iovino, and Q. Tang. Updatable functional encryption. In *Mycrypt 2016: Paradigm-shifting Crypto*, page ?? Springer, 2016.

[Conference28]V. Iovino, Q. Tang, and K. Zebrowski. On the power of public-key function-private functional encryption. In *Cryptology and Network Security - 15th International Conference, CANS 2016*, volume 10052 of *LNCS*, pages 585–593, 2016.

[Conference29]J. Lancrenon, M. Skrobot, and Q. Tang. Two more efficient variants of the J-PAKE protocol. In *Applied Cryptography and Network Security - 14th International Conference, ACNS 2016*, volume 9696 of *LNCS*, pages 58–76. Springer, 2016.

[Conference30]Q. Tang and B. Pejo. Poster: Game-theoretic framework for integrity verification in computation outsourcing. In *2016 Conference on Decision and Game Theory for Security*, page ?? springer, 2016.

[Conference31]Q. Tang, B. Pejo, and H. Wang. Protect both integrity and confidentiality in outsourcing collaborative filtering computations. In *2016 IEEE International Conference on Cloud Computing (CLOUD)*, page ?? IEEE, 2016.

[Conference32]J. Wang and Q. Tang. A probabilistic view of neighborhood-based recommendation methods. In *ICDM-2016 Workshop on Data Mining Systems and their Applications on the Cloud: CLOUDMINE*, page ?? IEEE, 2016.

Conference and Workshop (2013-2015)

[Conference33]M. Chenal and Q. Tang. Key recovery attack against an NTRU-type somewhat homomorphic encryption scheme. In *18-th Information Security Conference (ISC 2015)*, volume 9290 of *LNCS*, pages 1–22. Springer, 2015.

[Conference34]Q. Tang. Towards forward security properties for PEKS and IBE. In *Information Security and Privacy - 20th Australasian Conference (ACISP 2015)*, volume 9144 of *LNCS*, pages 127–144. Springer, 2015.

[Conference35]Q. Tang and J. Wang. Privacy-preserving context-aware recommender systems: Analysis and new solutions. In G. Pernul, P. Y. A. Ryan, and E. R. Weippl, editors, *Computer Security - ESORICS 2015*, volume 9327 of *LNCS*, pages 101–119. Springer, 2015.

[Conference36]A. Arriaga, Q. Tang, and P. Ryan. Trapdoor privacy in asymmetric searchable encryption schemes. In D. Pointcheval and D. Vergnaud, editors, *Progress in Cryptology – AFRICACRYPT 2014*, volume 8469 of *LNCS*, pages 31–50. Springer, 2014.

[Conference37]C. Bösch, A. Peter, B. Leenders, H. W.i Lim, Q. Tang, H.g Wang, P. H. Hartel, and W. Jonker. Distributed searchable symmetric encryption. In *2014 Twelfth Annual International Conference on Privacy, Security and Trust (PST)*, pages 330–337, 2014.

[Conference38]M. Chenal and Q. Tang. On key recovery attacks against existing somewhat homomorphic encryption schemes. In *Progress in Cryptology – LATINCRYPT 2014*, pages 239–258, 2014.

[Conference39]Q. Tang. Towards a privacy-preserving solution for osns. In J. Lopez, X. Huang, and R. Sandhu, editors, *Network and System Security - 7th International Conference (NSS 2013)*, volume 7873, pages 635–641. Springer, 2013.

[Conference40]Q. Tang and X. Chen. Towards asymmetric searchable encryption with message recovery and flexible search authorization. In *8th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2013)*, pages 253–264. ACM, 2013.

Conference and Workshop (2010-2012)

[Conference41]C. Bosch, Q. Tang, P. Hartel, and W. Jonker. Selective document retrieval from encrypted databse. In *Information Security Conference - 15th Information Security Conference (ISC 2012)*, volume 7483, pages 224–241. Springer, 2012.

[Conference42]X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou. New algorithms for secure outsourcing of modular exponentiations (extended abstract). In S. Foresti, M. Yung, and F. Martinelli, editors, *17th European Symposium on Research in Computer Security (ESORICS 2012)*, volume 7459, pages 541–556. Springer, 2012.

[Conference43]A. Jeckmans, Q. Tang, and P. Hartel. Privacy-preserving collaborative filtering based on horizontally partitioned dataset. In *2012 International Symposium on Security in Collaboration Technologies and Systems (CTS 2012)*, pages 439–446, 2012.

[Conference44]Q. Tang. Cryptographic framework for analyzing the privacy of recommender algorithms. In *2012 International Symposium on Security in Collaboration Technologies and Systems (CTS 2012)*, pages 455–462, 2012.

[Conference45]A. Jeckmans, Q. Tang, and P. Hartel. Privacy-preserving profile matching using the social graph. In *The Third International Conference on Computational Aspects of Social Networks (CASoN 2011)*, pages 42–47, 2011.

[Conference46]A. Jeckmans, Q. Tang, and P. Hartel. Privacy-preserving profile similarity computation in online social networks. In *Proceedings of the 18th ACM conference on Computer and communications security (CCS 2011)*, pages 793–796, 2011.

[Conference47]Q. Tang. Towards public key encryption scheme supporting equality test with fine-grained authorization. In *Proceedings of the 16th Australasian Conference on Information Security and Privacy (ACISP 2011)*, volume 6812 of *LNCS*, pages 389–406. Springer, 2011.

[Conference48]Z. Gong, Q. Tang, Y. W. Law, and H. Chen. Kalwen+: Practical key management schemes for gossip-based wireless medical sensor networks. In *Proceedings of the 6th China International Conference on Information Security and Cryptology (Inscrypt 2010)*, volume 6584 of *LNCS*, pages 268–283. Springer, 2010.

[Conference49]Q. Tang. Privacy preserving mapping schemes supporting comparison. In *Proceedings of the 2010 ACM workshop on Cloud computing security workshop (CCSW 2010)*, pages 53–58, 2010.

[Conference50]Q. Tang. User-friendly matching protocol for online social networks. In *Proceedings of the 17th ACM conference on Computer and communications security (CCS 2010)*, pages 732–734, 2010.

[Conference51]Q. Tang and A. Jeckmans. Efficient client puzzle schemes to mitigate DoS attacks. In *Proceedings of the 6th International Conference on Computational Intelligence and Security (CIS 2010)*, pages 732–734, 2010.

Conference and Workshop (2007-2009)

[Conference52]L. Ibraimi, Q. Tang, P. H. Hartel, and W. Jonker. Efficient and provable secure ciphertext-policy attribute-based encryption schemes. In F. Bao, H. Li, and G. Wang, editors, *Information Security Practice and Experience, 5th International Conference (ISPEC 2009)*, volume 5451 of *LNCS*, pages 1–12. Springer, 2009.

[Conference53]W. Pieters and Q. Tang. Data is key: Introducing the data-based access control paradigm. In E. Gudes and J. Vaidya, editors, *Data and Applications Security XXIII, 23rd Annual IFIP WG 11.3 Working Conference (DBSec 2009)*, volume 5645 of *LNCS*, pages 240–251. Springer, 2009.

[Conference54]Q. Tang. Timed-ephemerizer: Make assured data appear and disappear. In *Proceeding of Public Key Infrastructure, 5th European PKI Workshop: Theory and Practice (EuroPKI 2009)*, volume 6391 of *LNCS*, pages 195–208. Springer, 2009.

[Conference55]Q. Tang and L. Chen. Public-key encryption with registered keyword search. In *Proceeding of Public Key Infrastructure, 5th European PKI Workshop: Theory and Practice (EuroPKI 2009)*, volume 6391 of *LNCS*, pages 163–178. Springer, 2009.

[Conference56]J. Weng, Y. Yang, Q. Tang, R. H. Deng, X. Ding, and F. Bao. Efficient conditional proxy re-encryption scheme with chosen-ciphertext security. In *Information Security Conference - 12th Information Security Conference (ISC 2009)*, volume 5735 of *LNCS*, pages 151–166. Springer, 2009.

[Conference57]I. Buhan, J. Doumen, P. Hartel, Q. Tang, and R. Veldhuis. Embedding renewable cryptographic keys into continuous noisy data. In L. Chen, M. Ryan, and G. Wang, editors, *Information and Communications Security, 10th International Conference (ICICS 2008)*, volume 5308 of *LNCS*, pages 294–310. Springer, 2008.

[Conference58]T. Dimkov, Q. Tang, and P. Hartel. Inability of existing security models to cope with data mobility in dynamic organizations. In J. Whittle, J. Jrjens, B. Nuseibeh, and G. Dobson, editors, *Proceedings of Modeling Security Workshop (In Association with MODELS '08)*, volume 413. Sun SITE Central Europe, 2008. Available at http://ftp.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-413/.

[Conference59]L. Ibraimi, Q. Tang, P. Hartel, and W. Jonker. A type-and-identity-based proxy re-encryption scheme and its application in healthcare. In W. Jonker and M. Petkovic, editors, *Secure Data Management, 5th VLDB Workshop (SDM 2008)*, volume 5159 of *LNCS*, pages 185–198. Springer, 2008.

[Conference60]Q. Tang. Type-based proxy re-encryption and its construction. In D. R. Chowdhury and V. Rijmen, editors, *Proceeding of the 9th International Conference on Cryptology in India (Indocrypt 2008)*, volume 5365 of *LNCS*, pages 130–144. Springer, 2008.

[Conference61]Q. Tang, J. Bringer, H. Chabanne, and D. Pointcheval. A formal study of the privacy concerns in biometric-based remote authentication schemes. In L. Chen, Y. Mu, and W. Susilo, editors, *Information Security Practice and Experience, 4th International Conference (ISPEC 2008)*, volume 4991 of *LNCS*, pages 56–70. Springer, 2008.

[Conference62]Q. Tang, P. Hartel, and W. Jonker. Inter-domain identity-based proxy re-encryption. In M. Yung, P. Liu, and D. Lin, editors, *Proceeding of the 4th International Conferences on Information Security and Cryptology (Inscrypt 2008)*, volume 5487 of *LNCS*, pages 332–347. Springer, 2008.

[Conference63]J. Bringer, H. Chabanne, M. Izabachène, D. Pointcheval, Q. Tang, and S. Zimmer. An application of the goldwasser-micali cryptosystem to biometric authentication. In J. Pieprzyk, H. Ghodosi, and E. Dawson, editors, *Information Security and Privacy, 12th Australasian Conference (ACISP 2007)*, volume 4586 of *LNCS*, pages 96–106. Springer, 2007.

[Conference64]J. Bringer, H. Chabanne, D. Pointcheval, and Q. Tang. Extended private information retrieval and its application in biometrics authentications. In F. Bao, S. Ling, T. Okamoto, H. Wang, and C. Xing, editors, *Cryptology and Network Security, 6th International Conference (CANS 2007)*, volume 4856 of *LNCS*, pages 175–193. Springer, 2007.

[Conference65]J. Bringer, H. Chabanne, and Q. Tang. An application of the naccache-stern knapsack cryptosystem to biometric authentication. In *2007 IEEE Workshop on Automatic Identification Advanced Technologies*, pages 180–185, 2007.

[Conference66]A. W. Dent and Q. Tang. Revisiting the security model for timed-release encryption with pre-open capability. In J. A. Garay, A. K. Lenstra, M. Mambo, and R. Peralta, editors, *Information Security, 10th International Conference (ISC 2007)*, volume 4779 of *LNCS*, pages 158–174. Springer, 2007.

[Conference67]Q. Tang. On the security of three versions of the WAI protocol in chinese WLAN implementation plan. In *Proceedings of the Second International Conference on Communications and Networking in China (ChinaCom 2007)*, pages 333–339. IEEE, 2007.

Conference and Workshop (2003-2006)

[Conference68]Z. Cheng, L. Chen, R. Comley, and Q. Tang. Identity-based key agreement with unilateral identity privacy using pairings. In K. Chen, R. H. Deng, X. Lai, and J. Zhou, editors, *Information Security Practice and Experience, Second International Conference (ISPEC 2006)*, volume 3903 of *LNCS*, pages 202–213. Springer, 2006.

[Conference69]Q. Tang and K. R. Choo. Secure password-based authenticated group key agreement for data-sharing peer-to-peer networks. In J. Zhou, M. Yung, and F. Bao,

editors, *Applied Cryptography and Network Security, 4th International Conference (ACNS 2006)*, volume 3989 of *LNCS*, pages 162–177, 2006.

[Conference70]Q. Tang and C. J. Mitchell. Efficient compilers for authenticated group key exchange. In Y. Hao, J. Liu, Y. Wang, Y. Cheung, H. Yin, L. Jiao, J. Ma, and Y. Jiao, editors, *Computational Intelligence and Security, International Conference (CIS 2005)*, volume 3802 of *LNCS*, pages 192–197. Springer, 2005.

[Conference71]Q. Tang and C. J. Mitchell. On the security of some password-based key agreement schemes. In Y. Hao, J. Liu, Y. Wang, Y. Cheung, H. Yin, L. Jiao, J. Ma, and Y. Jiao, editors, *Computational Intelligence and Security, International Conference (CIS 2005)*, volume 3802 of *LNCS*, pages 149–154. Springer, 2005.

[Conference72]Q. Tang and C. J. Mitchell. Security properties of two authenticated conference key agreement protocols. In S. Qing, W. Mao, J. Lopez, and G. Wang, editors, *Information and Communications Security, 7th International Conference (ICICS 2005)*, volume 3783 of *LNCS*, pages 304–314. Springer, 2005.

[Conference73]Q. Tang. A new divisible anonymous off-line electronic payment system. In *Proceedings of the IASTED International Conference on Communication, Network, and Information Security*, 2003.

Technical Report

[Report74]E. Ayday, Q. Tang, and A. Yilmaz. Cryptographic solutions for credibility and liability issues of genomic data. http://eprint.iacr.org/2016/478, 2016.

[Report75]Q. Tang and H. Wang. Privacy-preserving hybrid recommender system. http://eprint.iacr.org/2016/1134, 2016.

[Report76]H. Wang and Q. Tang. Efficient homomorphic integer polynomial evaluation based on gsw fhe. http://eprint.iacr.org/2016/488, 2016.

[Report77]Q. Tang. On using encryption techniques to enhance sticky policies enforcement. Technical Report TR-CTIT-08-64, Centre for Telematics and Information Technology, University of Twente, 2008.

[Report78]Q. Tang. Key establishment protocols and timed-release encryption schemes. Royal Holloway, University of London, Mathematics Department Technical Report RHUL-MA-2007-9, 2007. PhD Thesis.

[Report79]C. J. Mitchell and Q. Tang. Cryptanalysis of a technique to transform discrete logarithm based cryptosystems into identity-based cryptosystems. Royal Holloway, University of London, Mathematics Department Technical Report RHUL-MA-2005-4, 2005.

[Report80]C. J. Mitchell and Q. Tang. Security of the Lin-Lai smart card based user authentication scheme. Royal Holloway, University of London, Mathematics Department Technical Report RHUL-MA-2005-1, 2005.

[Report81]Q. Tang and L. Chen. Weaknesses in two group Diffie-Hellman key exchange protocols. Cryptology ePrint Archive: Report 2005/197, 2005.

[Report82]Q. Tang and C. J. Mitchell. Cryptanalysis of an anonymous wireless authentication and conference key distribution scheme. Cryptology ePrint Archive: Report 2005/047, 2005.

[Report83]Q. Tang and C. J. Mitchell. Enhanced password-based key establishment protocol. Cryptology ePrint Archive: Report 2005/141, 2005.

[Report84]Q. Tang and C. J. Mitchell. Weaknesses in a leakage-resilient authenticated key transport protocol. Cryptology ePrint Archive: Report 2005/173, 2005.

[Report85]C. J. Mitchell and Q. Tang. Cryptanalysis of the Yeh-Sun password-based authentication protocols. Royal Holloway, University of London, Mathematics Department Technical Report RHUL-MA-2004-4, 2004.

[Report86]Q. Tang and C. J. Mitchell. Rethinking the security of some authenticated group key agreement schemes. Cryptology ePrint Archive: Report 2004/363, 2004.