CURRICULUM VITAE

Yongge Wang

(http://webpages.uncc.edu/yonwang/, https://en.wikipedia.org/wiki/Yongge_Wang)

1 Education

- 09/1988–07/1991 M.Sc. S.S.Chern Institute of Mathematics, Nankai University, China
- 10/1993–08/1996 Ph.D., magna cum laude. Computer science, Heidelberg University (Germany), Thesis title: Randomness and Complexity. Advisor: Prof. Dr. Klaus Ambos-Spies.

2 Professional Experience

- 07/2017– present: Full Professor at University of North Carolina at Charlotte
- 10/2014– present: Chief Security Officer at USMobile (http://www.usmobile-inc.com/about.html).
- 08/2015-07/2017: PhD track coordinator for SIS Department, UNC Charlotte
- 08/2007– 06/2017: Associate Professor at University of North Carolina at Charlotte
- 10/2014-06/2015: Visiting professor for cyber security at Qatar University
- 08/2008-07/2009: Graduate Coordinator at SIS Dept., UNC Charlotte
- 08/2002– 07/2007: Assistant Professor at University of North Carolina at Charlotte
- 07/1999–04/2000: Research associate at the CACR of University of Waterloo http://cacr.uwaterloo.ca
- 11/1997–06/1999: Research associate at University of Wisconsin at Milwaukee
- 01/1997–10/1997: Research associate at Auckland University (New Zealand)
- 09/1996–12/1996: Research associate at Max-Planck-Institute for computer science (Germany) (http://www.mpi-sb.mpg.de/)
- 05/2000—8/2001: Cryptologic mathematicians at Certicom Corp. (now a division of RIM/Blackberry)
- 10/2001–07/2002: Senior security specialist at the start-up company Karthika Technologies Inc.
- 02/1999–06/1999: Programmer at Medical College of Wisconsin.

3 Licenses and Certifications

CISSP (Certified Information Systems Security Professional) by ISC2

4 Career Highlights

The detailed career highlights will be included in the full package. The following is a high level summary:

1. I regularly publish research results in the most prestigious venues that include (but not limited): **IEEE Trans. Information Theory, SIAM J. Computing, J. Cryptology, Theoretical Computer Science, Crypto, Eurocrypt, IEEE ISIT, IEEE CCC**, etc. Among the 72 peer-reviewed publications, twenty (22) appeared in Tier-1 venues and fourteen (14) appeared in Tier-2 venues. Google scholar shows that my works have been cited for more than 1600 times (by August 10, 2016).
2. My research has important impact on the community. Some of my results in Algorithmic Information Theory (AIT) have become the fundamental theorems in most AIT graduate textbooks (see, e.g., http://www.springer.com/us/book/9780387955674). Specifically, my results characterizing the equivalence among Chaitin's Omega number, universal Turing machine halting probability, and algorithmic randomness is one of the classical results in modern effective randomness research.
3. My research results have REAL long-term impact on information technology industry. I am the inventor of Remote Password Authentication Protocol SRP5 which is included in IEEE 1363.2 standards and I am the inventor of identity based authentication protocol WANG-KE that is included in IEEE 1363.3 standard. IEEE 1363.x is a series of the most influential industrial standards for cryptographic techniques that are and will be used by the industry. Due to my contributions to IEEE 1363 community,

I am currently a voting member for IEEE1363 standards and I received IEEE 1363 service award two times. I am one of the designers for fundamental XML security techniques. Specifically, I was one of the contributors for designing XMLENC and XMLDSig syntax (http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/Overview.html). I am also one of the authors of IETF standard RFC 4050 on XML-Signature Syntax (https://tools.ietf.org/html/rfc4050). XMLENC/XMLDsig/RFC4050 are the starting point for all XML related security techniques.

4. I have been actively helping the industry to deliver secure products to protect the national infrastructure. DH-CHAP was originally proposed for standardization in IETF iSCSI working group. Due to my analysis and attacks, it was finally dropped from the standards. My post and follow-ups could be found at http://www.pdl.cmu.edu/mailinglists/ips/mail/msg09610.html. Cisco and AGA (American Gas Association) have been working on the SCADA communication security protocol for several years. After the representative (Dr. Andrew Wright) from Cisco visited UNC Charlotte seeking advice on the protocol. I broke the protocol within a few hours. Cisco and AGA had to re-design a new protocol.
5. I am the holder of three awarded patents (one Canadian patent, one World Intellectual Property Organization WIPO patent, and one US patent). I have been actively working on technology transfer and helped to start the secure communication company USMobile to commercialize NSA's Fishbowl project. I am currently serving as the Chief Security Officer for USMobile Inc. (http://www.usmobile-inc.com/about.html). I was one of the co-founders of UNC Charlotte spin off Calyptix Corp. (http://www.calyptix.com/).
6. I have been the inventor of Post-Quantum Cryptographic technique RLCE. The details of RLCE could be found at: http://quantumca.org . The RLCE technique has been submitted to NIST for Post-quantum cryptographic project as a candidate for NIST standards (http://csrc.nist.gov/groups/ST/post-quantum-crypto/) . I am the inventor and holder of three related US patent for RLCE techniques.
7. I actively serve the professional community by reviewing papers for prestigious journals, conferences, Mathematical Reviews, and by participating in prestigious funding panels.
8. I play leadership roles in developing research/education programs and in securing external research/education funding. Over last decades, by collaboration with colleagues (inside UNCC and outside of UNCC), we have collectively secured around US$8,331,400 funding for research and education. I play active roles in extending UNC Charlotte's interdisciplinary research and education. Collaborating with Prof. Dr. Ashit Talukder and researchers from UNCC and other institutes such as Caltech, JPL, RCN, we have just received a four-million-dollar project from NSF to design Data Infrastructure Building Blocks (DIBBs) to enhance UNC Charlotte's data science program.
9. As SIS department graduate and PhD coordinators, I have leaded the effort to re-certify the IT management certification program and leaded the effort to standardize SIS PHD track qualifying exam criteria. I have served as the Program Committee Chair for the 11th CCI annual security symposium (2010) to help the exposure of UNC Charlotte's Information Assurance program.
10. It is my highest priority to work with students on their research projects. I have supervised 21 senior project students, 15 master student theses/projects, and 3 PhD students. Among my 72 publications, ten (10) papers were collaborated with student co-authors (marked in the publication list). Among the 3 PhD students, one obtained his PhD degree (now at Facebook), one finished her qualifying exam, one is planning his qualifying exam. I have enjoyed my teaching and collaboration with students in classroom. My teaching evaluation is generally around the college and department average. I have leaded the effort to develop several new curriculums (e.g., cloud computing, open source technologies, software assurance and testing courses) in UNC Charlotte.

5 Publications

Note: I do not include acceptance rate since generally I do not keep tracks on that. Indeed, the most prestigious theory conferences such as STOC/FOCS generally have high acceptance rate (e.g., normally around 1/3) than applied technology venues. I do not include the citation information in this list

either since it changes frequently. The current citation information for my papers could be found at https://scholar.google.com/citations?user=GZtrefYAAAAJ&hl=en&oi=ao. By August 10, 2016, my papers have been **cited around 1600 times**, my **h-index is 20**, and my **i10-index is 39**.

5.1 Peer Reviewed Journal Publications (Summary: For journal papers, I have **twelve (12) tier 1** papers, **seven (7) tier 2** papers, **nine (9) tier 3** papers, and **four (4) tier 4** papers. **Four (4)** papers with student co-author)

- P.Li, X.Liu, X.Yi, Y.Wang and **Yongge Wang**. Brownian Motion Properties of Random Bit Generators Based on Laser Chaos. Optics Express 24(14):15822-15833. https://doi.org/10.1364/OE.24.015822 (**Tier 1.** impact factor: 3.148 for 2015)
- **Y. Wang** and Q. Malluhi and K.Khan: Garbled computation in cloud. Future Generation of Computer Systems, Vol 62, pages 54—65, 2015. https://doi.org/10.1016/j.future.2015.11.004 (**Tier 2**)
- **Y. Wang**: Privacy-preserving data storage in cloud using array BP-XOR codes. IEEE Transactions on Cloud Computing (TCC) 3(4):425--435, 2015. https://doi.org/10.1109/TCC.2014.2344662 (**Tier 1**)
- **Y. Wang** and T. Nicol: Statistical Properties of Pseudo Random Sequences and Experiments with PHP and Debian OpenSSL. Computers and Security (53):44-64, 2015 https://doi.org/10.1016/j.cose.2015.05.005 (**Tier 1**) [**with student co-author**]
- M. Paterson, D.R. Stinson, and **Y. Wang**. On encoding symbol degrees of array BP-XOR codes. Cryptography and Communications 8(1):19--32, 2016. https://doi.org/10.1007/s12095-015-0134-9 (**Tier 3**)
- **Y. Wang**. Efficient identity-based and authenticated key agreement protocol. Transactions on Computational Science, 17:172–197. 2013. https://doi.org/10.1007/978-3-642-35840-1_9 (**Tier 3**)
- Tozal, M. E., **Wang, Y**., Al-Shaer, E., Sarac, K., Thuraisingham, B. M., and Chu, B. Adaptive information coding for secure and reliable wireless telesurgery communications. MONET, 18(5):697–711, 2013. https://doi.org/10.1007/s11036-011-0333-3 (**Tier 2**) [**with student co-author**]
- J. Xia and **Y. Wang**. Secure key distribution for the smart grid. IEEE Trans. Smart Grid, 3(3):1437–1443, 2012. https://doi.org/10.1109/TSG.2012.2199141 (**Tier 1**) [**with student co-author**].
  Comments on this paper: when the student worked with me, I gave him a complete protocol design idea and asked the student to finish the paper. At the time when the student finished the paper and submitted the paper to the journal, he had switched advisor thus he did not ask me to read the paper. The student misunderstood my design and did not include user name in the final key calculation process. Thus the published protocol was not my original protocol and is insecure. A colleague has pointed out this error to me already.
- **Y. Wang** and Y. Desmedt. Edge-Colored Graphs with Applications To Homogeneous Faults. Information Processing Letters 111:634–641, 2011. https://doi.org/10.1016/j.ipl.2011.03.017 (**Tier 2**)
- **Y. Wang**. sSCADA: securing SCADA infrastructure communications. Int. J. Communication Networks and Distributed Systems. 6(1):59–78, 2011. https://doi.org/10.1504/IJCNDS.2011.037328 (**Tier 3**)
- **Y. Wang** and Y. Desmedt. Perfectly Secure Message Transmission Revisited. IEEE Transaction on Information Theory. 54(6):2582–2595, June 2008. https://doi.org/10.1109/TIT.2008.921676 (**Tier 1**)
- X. Wu, Y. Wang, S. Guo, and Y. Zheng (2007). Privacy preserving database generation for database application testing. Fundamenta Informaticae, 78(4), 595-612. http://content.iospress.com/articles/fundamenta-informaticae/fi78-4-09 (**Tier 3**) [**with student co-author**]
- Z. Zhao, Z. Dong, and **Y. Wang**. Security Analysis of a Password-Based Authentication Protocol Proposed to IEEE 1363. Theoretical Computer Science. 352(1-3):280–287, 2006. https://doi.org/10.1016/j.tcs.2005.11.038 (**Tier 1**)
- **Y. Wang**. Robust key establishment in sensor networks. ACM SIGMOD Record 33(1):14–19, March, 2004. https://doi.org/10.1145/974121.974124 (**Tier 1**)
- Y. Desmedt and **Y. Wang**. Analyzing vulnerabilities of critical infrastructures using flows and critical vertices in AND/OR graphs. International Journal of Foundations of Computer Science, 15(1):107–125, World Scientific Press, 2004. https://doi.org/10.1142/S0129054104002339 (**Tier 3**)
- **Y. Wang**. A comparison of two approaches to pseudorandomness. Theoretical Computer Science 276(1-2):449–459, 2002. https://doi.org/10.1016/S0304-3975(01)00311-5 (**Tier 1**)
- **Y. Wang**. The algebraic structure of the isomorphic types of tally polynomial time sets. Archive for Mathematical Logic 41(3): 215–244, 2002. https://doi.org/10.1007/s001530100117 (**Tier 2**)

- W. Merkle and **Y. Wang**. Separations by random oracles and almost-classes for generalized reducibilities. Mathematical Logic Quarterly 47(2):249–269, 2001. https://doi.org/10.1002/1521-3870(200105)47:2<249::AID-MALQ249>3.0.CO;2-N (**Tier 3**)
- **Y.Wang** and Y.Desmedt. Secure communication in multicast channels. Journal of Cryptology 14(2):121–135, 2001. https://doi.org/10.1007/s00145-001-0002-y (**Tier 1**)
- C. Calude, P. Hertling, B. Khoussainov, and **Y. Wang**. Recursively enumerable reals and Chaitin's Ω numbers. Theoretical Computer Science 255:125–149, 2001. https://doi.org/10.1016/S0304-3975(99)00159-0 (**Tier 1**)
- **Y. Wang**, Y. Desmedt, and M. Burmester. Models for dependable computation with multiple inputs and some hardness results. Fundamenta Informaticae 42(1):61–73, 2000. https://doi.org/10.3233/FI-2000-42103 (**Tier 3**)
- **Y. Wang**. Resource bounded randomness and computational complexity. Theoretical Computer Science 237(1-2):33–55, 2000. https://doi.org/10.1016/S0304-3975(98)00119-4 (**Tier 1**)
- **Y. Wang**. Genericity, Randomness, and Polynomial-Time Approximations. SIAM Journal on Computing 28(2):394-408, 1999. https://doi.org/10.1137/S009753979630235X (**Tier 1**)
- **Y.Wang**. A separation of two randomness concepts. Information Processing Letters,69(3):115–118, 1999. https://doi.org/10.1016/S0020-0190(98)00202-6 (**Tier 2**)
- **Y. Wang**: Randomness, stochasticity, and approximations. Theory of Computing Systems, 32:517–529, 1999. https://doi.org/10.1007/s002240000130 (**Tier 2**)
- **Y. Wang**. Abuses of probabilistic encryption schemes. IEE Electronics Letters, 34(8):753–754, 1998. https://doi.org/10.1049/el:19980496 (**Tier 3**)
- P. Hertling and **Y. Wang**. Invariance properties of random sequences. Journal of Universal Computer Science, 3(11):1241-1449, 1997. https://doi.org/10.3217/jucs-003-11-1241 (**Tier 3**)
- **Y. Wang**. NP-hard sets are superterse unless NP is small. Information Processing Letters 61(1):1-6, 1997. https://doi.org/10.1016/S0020-0190(96)00189-5 (**Tier 2**)
- **Y. Wang**. Modified data-flow models and their applications. Chinese Journal of Software, 5(3):43-48, 1994. http://www.cnki.com.cn/Article/CJFDTotal-RJXB403.005.htm (**Tier 4**)
- G. Hu and **Y. Wang**. The fundamental theory for object-oriented languages. Chinese Journal of Computer Science, 20(4):1-6, 1993. (**Tier 4**)
- **Y. Wang**. The computing power of ordered Petri nets. Chinese Journal of Software, 4(3):35- 41, 1993. http://www.jourlib.org/paper/1704688#.VyEH_eb2aUk (**Tier 4**)
- S.Xu and **Y.Wang**. Blum's speed up theorem and the hierarchy of recursive functions. Chinese Journal of Software, 4(4):38-43, 1993. http://www.cnki.com.cn/Article/CJFDTotal-RJXB199304006.htm (**Tier 4**)

5.2 Peer Reviewed Conference Publications (Summary: for conference publications, I have **ten (10) tier-1** papers, **seven (7) tier-2** papers, **seventeen (17) tier-3** papers, and **six (6) tier-4** papers. **Six (6)** papers with student co-author)

- **Y. Wang** (2017). Secure Communication and Authentication Against Off-line Dictionary Attacks in Smart Grid Systems. In: Cuppens-Boulahia N., Lambrinoudakis C., Cuppens F., Katsikas S. (eds) Security of Industrial Control Systems and Cyber-Physical Systems. CyberICPS 2016. Lecture Notes in Computer Science, vol 10166. Pages 103-120. Springer, https://doi.org/10.1007/978-3-319-61437-3_7
- Khaled Khan, Mahboob Shaheen, and **Yongge Wang**. Data Confidentiality in Cloud-based Pervasive System. Proc. ACM 2nd International Conference on Internet of Things, Data and Cloud Computing 2017.
- **Y. Wang**. and Q.M. Malluhi (2016). Privacy Preserving Computation in Cloud Using Noise-Free Fully Homomorphic Encryption (FHE) Schemes. In Proc. ESORICS 2016, LNCS 9878, pp. 301-323. https://doi.org/10.1007/978-3-319-45744-4_15 (**Tier 1**)
- **Y. Wang**: Quantum Resistant Random Linear Code Based Public Key Encryption Scheme RLCE. In Proc. IEEE ISIT 2016, pages 2519-2523. http://dx.doi.org/10.1109/ISIT.2016.7541753 (**Tier 1**)
- **Y. Wang** and Y. Desmedt. Efficient Secret Sharing Schemes Achieving Optimal Information Rate. In IEEE Information Theory Workshop (ITW), pages 516—520, 2014. https://doi.org/10.1109/ITW.2014.6970885 (**Tier 2**)
- **Y. Wang** and T. Nicol: Statistical Properties of Pseudo Random Sequences and Experiments with PHP and Debian OpenSSL. In ESORICS 2014, LNCS 8712, pp. 454--471. 2014. https://doi.org/10.1007/978-3-319-11203-9_26 (**Tier 1**) [**with student co-author**]

- **Y. Wang**. Array BP-XOR codes for reliable cloud storage systems. In Proc IEEE ISIT 2013, pages 326–330. IEEE Press. 2013. https://doi.org/10.1109/ISIT.2013.6620241 (**Tier 1**)
- Duan, Q., **Wang, Y**., Mohsen, F., and Al-Shaer, E. Private and anonymous data storage and distribution in cloud. In Services Computing (SCC), 2013 IEEE International Conference on, pages 264–271. IEEE. 2013. https://doi.org/10.1109/SCC.2013.53 (**Tier 3**) [**with student co-author**]
- **Wang, Y.** Password protected smart card and memory stick authentication against off-line dictionary attacks. In SEC IFIP AICT 376, pages 489–500. 2012. https://doi.org/10.1007/978-3-642-30436-1_40 (**Tier 3**)
- Tozal, M. E., **Wang, Y**., Al-Shaer, E., Sarac, K., Thuraisingham, B. M., and Chu, B. (2011). On secure and resilient telesurgery communications over unreliable networks. In INFOCOM Cyber-Physical Networking Systems (CPNS), pages 714–719. IEEE Computer Society Press. 2011. https://doi.org/10.1109/INFCOMW.2011.5928905 (**Tier 3**) [**with student co-author**]
- **Y. Wang** and Y. Desmedt. Homogeneous Faults, Colored Edge Graphs, and Cover Free Families. In Proc. 5th International Conference on Information Theoretic Security (ICITS 2011), pages 58-72. LNCS 6673. https://doi.org/10.1007/978-3-642-20728-0_6 (**Tier 3**)
- M. Boujettif and **Y.Wang**. Constructivist Approach To Information Security Awareness In The Middle East. In: Proc. 2010 Int. Conf. Broadband, Wireless Computing, Communication and Applications (BWCCA), pp.192-199, IEEE Press 2010. https://doi.org/10.1109/BWCCA.2010.70 (**Tier 4**) [**with student co-author**]
- Y. Desmedt, **Y. Wang** and M. Burmester. Revisiting Colored Networks and Privacy Preserving Censorship. Proc. 1st International Workshop on Critical Information Infrastructures Security (CRITIS'06) August 30 - September 2, 2006, Greece. LNCS 4347, pages 140-150, 2006. https://doi.org/10.1007/11962977_12 (**Tier 3**)
- Y. Desmedt and **Y. Wang**. Survey of Models for Critical Infrastructures and Methods to Measure Robustness. Proc. of the first CRIS International Workshop on Critical Information Infrastructures (CIIW'05). http://www.ida.liu.se/conferences/CIIW05/program.shtml (**Tier 4**)
- Y. Desmedt, **Y. Wang** and M. Burmester. A complete characterization of tolerable adversary structures for secure point-to-point transmissions. In Proc. 16th ISAAC, LNCS 3827, pages 277-287, 2005. https://doi.org/10.1007/11602613_29 (**Tier 2**)
- **Y. Wang** and X. Wu. Approximate inverse frequent itemset mining: privacy, complexity, and approximation. In Proc. 5th IEEE ICDM (ratio: 69/630). pages 482-489, 2005. https://doi.org/10.1109/ICDM.2005.27 (**Tier 2**)
- Y. Zheng and **Y. Wang**. Efficient and provably secure ciphers for storage device block level encryption. In Proc. ACM StorageSS Workshop. Pages 103-107, 2005. https://doi.org/10.1145/1103780.1103796 (**Tier 3**)
- X. Wu, C. Sanghvi, **Y. Wang**, and Y. Zheng. Privacy aware data generation for testing database applications. Proc. of Ninth International Database Engineering and Applications Symposium (IDEAS 2005), pages 317–326, IEEE Press. https://doi.org/10.1109/IDEAS.2005.45 (**Tier 3**) [**with student co-author**]
- Y.Desmedt, **Y.Wang**, R.Safavi-Naini, and H.Wang. Radio networks with reliable communications. In Proc. COCOON 05, LNCS 3595, pages 156–166, August 2005. https://doi.org/10.1007/11533719_18 (**Tier 3**)
- X. Wu, Y. Wu, **Y. Wang**, and Y. Li. Privacy aware market basket data set generation: a feasible approach for inverse frequent set mining. In Proc. 5th SIAM International Conference on Data Mining, April 2005. https://doi.org/10.1137/1.9781611972757.10 (**Tier 2**) [**with student co-author**]
- X.Wu, **Y.Wang**, and Y.Zheng. Statistical Database Modeling for Privacy Preserving Database Generation. In: Proc. 15th International Symposium on Methodologies for Intelligent Systems (New York), LNCS 3488, Pages 382–390, Springer, 2005. https://doi.org/10.1007/11425274_40 (**Tier 3**)
- **Y. Wang**, X. Wu, and Y. Zheng. Privacy preserving data generation for database application performance testing. In: Proc. 1st International Conference on Trust and Privacy in Digital Business (TrustBus '04, together with DEXA) (Eds. Sokratis Katsikas, Javier Lopez, Guenther Pernul) LNCS 3184, pages 142-151, 2004, Springer-Verlag. https://doi.org/10.1007/978-3-540-30079-3_15 (**Tier 3**)
- M. Burmester, Y. Desmedt, and **Y. Wang**. A Critical analysis of models for fault-tolerant and secure computation. In: Proceedings of the IASTED Communication, Network, and Information Security (CNIS), 2003, pages 147-152. https://www.scopus.com/record/display.uri?eid=2-s2.0-2642526975&origin=inward&txGid=0 (**Tier 4**)

- **Y. Wang** and Y. Zheng. Fast and secure WORM storage systems. In: Proceedings of the IEEE Security in Storage Workshop (SISW), pages 11-19, 2003, IEEE Press. https://doi.org/10.1109/SISW.2003.10002 (**Tier 3**)
- X. Wu, **Y. Wang**, and Y. Zheng. Privacy preserving database application testing. In: Proc. of the ACM Workshop on Privacy in Electronic Society, pages 118–128, 2003, ACM Press. https://doi.org/10.1145/1005140.1005159 (**Tier 3**)
- Z. Liu and **Y. Wang**. A secure agent architecture for sensor networks. In Proc. 2003 International Conference on Artificial Intelligence–Intelligent Pervasive Computing Workshop (IC-AI'03 June 23-26, 2003, Las Vegas, Nevada, USA), pages 10–16, 2003, CSREA Press. (**Tier 4**)
- **Y. Wang**, Y. Zheng, and B. Chu: Efficient and secure storage systems based on peer-to-peer systems. In Proc. 2003 International Conference on Artificial Intelligence- Intelligent Pervasive Computing Workshop (IC-AI'03 June 23-26, 2003, Las Vegas, Nevada, USA), pages 17–22, 2003, CSREA Press. (**Tier 4**)
- Y. Desmedt and **Y. Wang**. Efficient Zero-knowledge proofs for some practical graph problems. In Proceedings of Third Conference on Security in Communication Networks, Lecture Notes in Computer Science 2576, pages 296–308, 2002. https://doi.org/10.1007/3-540-36413-7_21 (**Tier 3**)
- Y. Desmedt and **Y. Wang**. Maximum Flows and Critical Vertices in AND/OR Graphs. In Proc. COCOON '02, pages 238-248. Lecture Notes in Computer Science 2387, Springer-Verlag. Preliminary results were presented at INFORM '99 Cincinnati, section SA34.1. https://doi.org/10.1007/3-540-45655-4_27 (**Tier 3**)
- Y. Desmedt and **Y. Wang**: Perfectly Secure Message Transmission Revisited. In Proc. EuroCrypt'02, pages 502-517. LNCS 2332, Springer-Verlag. https://doi.org/10.1007/3-540-46035-7_33 (**Tier 1**)
- S. Blake-Wilson, A. Menezes, R. Struik and **Y. Wang**. Security Issues with Practical Realizations of the Ideal Cipher Model. In Proc. Crypt'01. Springer-Verlag. https://www.iacr.org/conferences/crypto2001/accepted.htm (**Tier 1**)
  This paper was accepted for inclusion in the proceedings of Crypto 2001 and was presented at Crypto 2001. My employer (Certicom) preferred to have a trade secret on the technique. Thus Certicom asked the conference not to include the full paper in the final conference proceedings.
- **Y. Wang**. Using mobile agent results to create hard-to-detect computer viruses. In Information Security for Global Information Infrastructures, the 16th IFIP SEC (2000), pages 161–170, Kluwer Academic Publishers. http://dl.acm.org/citation.cfm?id=719496 (**Tier 3**)
- **Y. Wang**. Linear complexity versus pseudorandomness: on Beth and Dai's result. In Advances in Cryptology, Proc. of Asiacrypt 99, pages 288–298. Lecture Notes in Computer Science 1716, Springer Verlag. https://doi.org/10.1007/978-3-540-48000-6_23 (**Tier 1**)
- Y. Desmedt and **Y. Wang**. Approximation hardness and secure communication in broadcast channels. In Advances in Cryptology, Proc. Asiacrypt 99, pages 247–257. Lecture Notes in Computer Science 1716, Springer Verlag. https://doi.org/10.1007/978-3-540-48000-6_20 (**Tier 1**)
- **Y.Wang** and Y.Desmedt. Secure communication in multicast channels: the answer to Franklin and Wright question. In Advances in Cryptology, Proc. of Eurocrypt 99, pages 443–455. Lecture Notes in Computer Science 1592, Springer Verlag. https://doi.org/10.1007/3-540-48910-X_31 (**Tier 1**)
- C. Calude, P. Hertling, B. Khoussainov, and **Y. Wang**. Recursively enumerable reals and Chaitin's Ω numbers. In Proceedings of the 15th STACS, pages 596–606. Lecture Notes in Computer Science 1373, Springer Verlag, 1998. https://doi.org/10.1007/BFb0028594 (**Tier 2**)
- M. Burmester, Y. Desmedt, and **Y. Wang**: Using approximation hardness to achieve dependable computation. In Proc. of RANDOM 98, pages 172-186. Lecture Notes in Computer Science 1518, Springer Verlag. https://doi.org/10.1007/3-540-49543-6_15 (**Tier 3**)
- **Y. Wang**. Randomness, stochasticity, and approximations. In Proceedings of RANDOM 97 (Italy), pages 213–225. Lecture Notes in Computer Science 1269, Springer Verlag. https://doi.org/10.1007/3-540-63248-4_18 (**Tier 3**)
- **Y. Wang**. The law of the iterated logarithm for p-random sequences. In Proc. 11th IEEE Conference on Computational Complexity (CCC), pages 180-189. IEEE Computer Society Press, 1996. https://doi.org/10.1109/CCC.1996.507680 (**Tier 1**)
- K. Ambos-Spies, E. Mayordomo, **Y. Wang**, and X. Zheng. Resource bounded balanced genericity, stochasticity and weak randomness. In Proc. 13rd STACS '95, pages 63-74. Lecture Notes in Computer Science 1046, Springer Verlag. https://doi.org/10.1007/3-540-60922-9_6 (**Tier 2**)
- W. Merkle and **Y. Wang**. Separations by random oracles and almost-classes for generalized

reducibilities. In Proceedings of 20th MFCS. Lecture Notes in Computer Science 969, pages 179-190, 1995. https://doi.org/10.1007/3-540-60246-1_124 (**Tier 2**)

- G.Hu and **Y.Wang**. An algorithm and its data structure from sequential USMMCM to parallel machine. In Computer Mathematics, pages 58-65, World Sci. Publishing, River Edge, NJ, 1993 (MR: 94m:68041). (**Tier 4**)

5.3 Peer Reviewed Extended Abstracts/Short Papers (N/A)

5.4 Peer Reviewed Posters (N/A)

5.5 Peer Reviewed Books and Book Chapters

- **Y. Wang**. PKCS: Public-Key Cryptography Standards. In Handbook of Information Security (editor: Dr. Bidgoli), John Wiley & Sons, Inc., 2005. http://www.wiley.com/WileyCDA/Section/id-290006.html
- **Y. Wang**. Smart grid, automation, and SCADA systems security. In Xiao, Y., editor, Security and Privacy in Smart Grids, pages 245–268. CRC Press, 2013. https://www.crcpress.com/Security-and-Privacy-in-Smart-Grids/Xiao/9781439877838

5.6 Patents Awarded

- Thanos, D., Kent, C., and **Wang, Y**. (2003). Authentication protocols for networked storage devices. Publication number: CA2375898 A1. Publication date: Sep 11, 2013. Priority date: Mar 11, 2002. http://google.com/patents/CA2375898A1?cl=un
- **Wang, Y**., Kent, C., and Thanos, D. (2003a). System and method for authenticating components of a storage network. Publication number: WO2003077471 A1. Publication date: Sep 18, 2003. http://google.com/patents/WO2003077471A1?cl=sv
- **Wang, Y**. Systems and methods for performing randomness and pseudorandomness generation, testing, and related cryptographic techniques. Publication date: July 16, 2015. US Patent number: US20150199175 A1. http://www.google.ch/patents/US20150199175

5.7 Manuscripts under Review

- **Y. Wang**. and Y. Desmedt (2016a). Towards fully homomorphic encryption schemes from codes. Submitted.
- **Y. Wang**. and Q.M. Malluhi (2016b). Practical reusable garbled oblivious RAMs. Submitted.
- **Y. Wang**. and Q.M. Malluhi (2016c). Reducing Garbled Circuit Size While Preserving Circuit Gate Privacy. Submitted
- Mikhail Atallah, Chris Clifton, Qutaibah Malluhi and **Yongge Wang** (2016). Garbled Computations: Hiding Software, Data, and all Computed Values. Submitted

5.8 Patents under Review

- **Y. Wang**. Method and system for storing user credentials in a mobile device enabling single sign on without a trusted third party. Filing date: December 8, 2014. US Patent Application number: 62/088699
- **Y. Wang**. Method and apparatus for random linear code based public key encryptions schemes. Filing date: October 25, 2015. US Patent Application number: 62/240182

5.9 Other Publications

- Y. Desmedt, M. Burmester, and **Y. Wang**. Are we on the right track to achieve survivable computer networks. Presented at: Fourth IEEE/CERT Information Survivability Workshop (ISW-2001/2002)
- **Y.Wang** and Yvo Desmedt. Impediments to Achieving Survivable Systems", 2001. http://www.cert.org/research/isw/isw2001/papers/Desmet-03-09.pdf and http://www.cert.org/research/isw/isw2001/slides/ISW-right-track.pdf
- Y. Desmedt, M. Burmester, and **Y. Wang**. Using economics to model threats and security in distributed computing. Presented at Workshop on Economics and Information Security by University of California

at Berkeley, 2002.
http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/slides/desmedt.ppt
- A. Menezes, M. Qu, D. Stinson, and **Y. Wang**. Evaluation of Security Level of Cryptography: ACE Signature Scheme. Evaluation report for Japanese government IPA CRYPTREC project. http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1049_ace.pdf
- A. Menezes, M. Qu, D. Stinson, and **Y. Wang**. Evaluation of Security Level of Cryptography: ESIGN Signature Scheme. Evaluation report for Japanese government IPA CRYPTREC project. http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1053_esign.pdf
- A. Menezes, M. Qu, D. Stinson, and **Y. Wang**. Evaluation of Security Level of Cryptography: ESIGN Identification Scheme. Evaluation report for Japanese government IPA CRYPTREC project. http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1077_esigni.pdf
- A. Menezes, M. Qu, D. Stinson, and **Y. Wang**. Evaluation of Security Level of Cryptography: MY-ELLTY Signature Scheme. Evaluation report for Japanese government IPA CRYPTREC project. http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1055_ellty.pdf
- A. Menezes, M. Qu, D. Stinson, and **Y. Wang**. Evaluation of Security Level of Cryptography: ECDSA Signature Scheme. Evaluation report for Japanese government IPA CRYPTREC project.
- **Y.Wang**. DH-CHAP was originally proposed to IETF IPS working group as a password based authentication protocol for iSCSI. Due to my analysis and attacks, it was finally dropped from the standards. See my original post and follow-ups at: http://www.pdl.cmu.edu/mailinglists/ips/mail/msg09610.html
- **Y.Wang**. Inventor of SRP5 (Secure Remote Password Protocol 5) which is included in the IEEE 1363.2: "Standard Specifications For Public-Key Cryptography". http://grouper.ieee.org/groups/1363/passwdPK/index.html
- **Y.Wang**. Inventor of WANG-KE, included in IEEE1363.3 standards
- **Y.Wang** and others. "ECDSA with XML DSIG" IETF Request for Comments (RFC) 4050. http://www.ietf.org/rfc/rfc4050
- **Y.Wang**. Author of ANSI X9.92 draft: Public Key Cryptography For The Financial Services Industry: PV-Digital Signature Scheme Giving Partial Message Recovery
- Y.Wang. Cryptographic Challenges In Smart Grid System Security IEEE Smart Grid Newsletter, December, 2012. (http://smartgrid.ieee.org/newsletters/december-2012/cryptographic-challenges-in-smart-grid-system-security?highlight=WyJ5b25nZ2UiXQ==)

6 Extramural Funding

6.1 Peer Reviewed National and International Grants

- 2002.09–2003.08: G. Ahn (PI), B. Chu, T. Dahlberg, Z. Liu, W. Tolone, **Yongge Wang**, and Y. Zheng. "DoD Carolinas Cyber-Defender Scholarship Program" supported by DoD IASP. Amount **US$350,418**.
- 2002.09-2005.08: B. Chu (PI), G. Ahn, T. Dahlberg, Z. Liu, W. Tolone, **Yongge Wang**, Y. Zheng. NSF Carolina Cyber Defender Scholarship" by NSF. Amount: **US$2,004,112**
- 2003.09–2004.08: G. Ahn (PI), B. Chu, T. Dahlberg, S. Lee, Z. Liu, W. Tolone, **Yongge Wang**, D. Wilson, and Y. Zheng "DoD Carolinas Cyber-Defender Scholarship Program" supported by DoD IASP. Amount **US$201,460**.
- 2003.09–2006.08: Xintao Wu (PI), **Yongge Wang**, Yuliang Zheng: "Privacy preserving database application testing" supported by NSF CCR-0310974. Amount **US$230,800**.
- 2003.01-2004.01: B. Chu (PI), G. Ahn, T. Dahlberg, Z. Liu, W. Tolone, **Yongge Wang**, Y. Zheng. Department of Defense Information Assurance Scholarship Program" by DoD. Amount: **US$19,028**
- 2004.09-2006.09: B. Chu (PI), G. Ahn, S. Lee, Z. Liu, A. Raja, W. Tolone, **Yongge Wang**, D. Wilson, and Y. Zheng. Collaborative Project: Bridging Gaps in IA Education through Collaboration" by NSF, Amount: **US$300,000**
- 2004.09-2005.09: G. Ahn (PI), B. Chu, T. Dahlberg, S. Lee, Z. Liu, A. Raja, W. Tolone, **Yongge Wang**, D. Wilson, and Y. Zheng. DoD Carolinas Cyber-Defender Scholarship Program" by DoD IASP. Amount: **US$58,088**
- 2005.09-2006.09: G. Ahn (PI), B. Chu, T. Dahlberg, S. Lee, Z. Liu, A. Raja, W. Tolone, **Yongge Wang**, D. Wilson, and Y. Zheng. DoD Carolinas Cyber-Defender **Scholarship** Program" by DoD IASP. Amount: **US$60,016**

- 2016.05-2019.04: **Yongge Wang (Lead PI),** Qutaibah M. Malluhi, Yvo Desmedt, and Yuliang Zheng. "Efficiently Reliable and Privacy Preserving Cloud Data Storage" supported by Qatar Foundation -- NATIONAL PRIORITY RESEARCH PROGRAM - NPRP No.: NPRP8-2155-1-423. Amount **US$810,007**. (Approximately US$140,000 will be spent in UNC Charlotte as sub-contract). After I returned to UNC Charlotte, I transferred the LPI role in Qatar University part to Prof. Malluhi.
- 2016.10-2020.9. Ashit Talukder (PI), Wlodek Zadrozny, Wenwen Dou, Yongge Wang, Ehab Al-Shaer, William Tolone, Mirsad Hadzikadic. Data Infrastructure Building Blocks (DIBBs). US$3,999,531
- 2017.01-2019.12 Pu Li (PI), **Yongge Wang**, and several other co-PIs in China. Analyzing Brownian properties of chaotic sequences generated by laser (用布朗运动分析混沌密码的随机性). Funded by Chinese Bureau of Cryptography (国家密码管理局), "十三五"国家密码发展基金密码理论课题. CNY100,000.
- 2018.01-2021.12 Pu Li (PI), **Yongge Wang**, and several other co-PIs in China. Investigating randomness properties of chaotic signal with a high 3-dB bandwidth (基于超宽带激光相位混沌的高速物理随机数实时产生研究). Funded by Chinese National Science Foundation (国家自然科学基金委员会). CNY610,000.

6.2 Peer Reviewed Industrial Grants

- 01/2003–08/2003: **Yongge Wang**. "Strategic Plans for Secure Storage Systems" supported by Bank of America. Amount **US$43,939**.
- 09/2005–02/2006: Bill Chu, Gail Anh, **Yongge Wang**, Brent Kang. "Honeynet Research and Experience" supported by Bank of America. Amount **US$50,000**.

6.3 Peer Reviewed Regional Grants (N/A)

6.4 Peer Reviewed Institutional Grants

- 01/2004–06/2004: **Yongge Wang** "Faculty Research Grants" supported by UNC Charlotte. Amount **US$4300**.
- 01/2005–06/2005: **Yongge Wang** "Curriculum and Instructional Development Grant" supported by UNC Charlotte. Amount **US$5100**.
- 01/2006–06/2006: **Yongge Wang** "Faculty Research Grants" supported by UNC Charlotte. Amount **US$6000**.

6.5 Awards and Donations

- IEEE 1363.2 service award (2008)
- IEEE 1363.3 service award (2011)

6.6 Other Grants (N/A)

7 Student Supervision

7.1 Doctoral Students Supervised (graduated one, currently advising three)

- Libin Bai (graduated):
  PhD Dissertation title: Performance Optimization of Remote Networked Control Systems. Defense date: March 14, 2014 (at Facebook now).
  This student is co-advised with Prof. Sheng-Guo Wang from College of Engineering. Part of the funding was from Prof. Sheng-Guo Wang and part of the funding was from me. The student officially belongs to SIS PhD track
- Lida Safarnejad (passed QE and plans Proposal Defense):
  PhD Dissertation title: Privacy preserving cloud database.
  Lida passed QE on April 22, 2016. She is planning for proposal defense now.

- Eduardo Eckmann (passed QE):
  Eduardo was in his second year of PhD study.

7.2 Masters Students Supervised (including Master thesis)

- Abhishek Ballabh (Msc Thesis 2010): Thesis Title: Implementations of SRP5
- Ashish Vijaywargiya (2003 Spring and Fall): Project Title: Analysis of Security Mechanisms for SAN
- Anita Sehgal (2003-2004): Thesis: Simulation of a robust key establishment protocol for sensor networks
- Hariharan Venkatasubramanian (2004 Spring): Security testing of a commercial software package
- Atish Ashokkumar Shah (2004 Fall): Thesis Title: Classification of Attacks on Web services
- Yonge Ye (May to June 2003): NAS security for Bank of America. Supported by BoA project (EBTI)
- Gautam Singaraju (11.2002--02.2003): HESS implementation (a disk encryption algorithm).
- Kaushal Shah (May 2004): Polymorphic virus analysis
- Yu-Lin (Ula) Hsieh (May 2004): Polymorphic virus detection
- Krishnan Kesavaram: database encryption tools development 2005 May
- Ron Gilson: Buffer overflow flashing demonstration, 2005 May, supported by UNCC CID project
- Daniel Tong: Identity Based Crypto toolkits, 2005 May
- For certain period of 2005, I was also involved in the cyber-cop student spyware project supervision
- Roopesh Uppala: Proxy detection 2006 Fall
- Janani Venkataramani: Quality Assurance design and planning for Family Dollar, 2007 Spring

7.3 Bachelors Students Supervised (Senior projects)

- William Christopher Kees (2003 Spring and Fall): "remote storage system for wireless devices"
- Robert Brian Lockwood (2003 Spring and Fall): "remote storage system for wireless devices"
- Johnathan Lee Moore (2003 Spring and Fall): "remote storage system for wireless devices"
- Bradley Michael Reavis (2003 Spring and Fall): "remote storage system for wireless devices"
- Jason Matthew Allen (2003 Fall and 2004 Spring): "security analysis for peer to peer networks"
- Michael Brian Dickerson (2003 Fall and 2004 Spring): "security analysis for peer to peer networks"
- Roman Pyzh (2003 Fall and 2004 Spring): "security analysis for peer to peer networks"
- Chung K Tran (2003 Fall and 2004 Spring): "security analysis for peer to peer networks"
- Dimitre Todorov Stanimirov (2003 Fall and 2004 Spring): "cryptographic interface design"
- Aman Mayson (2003 Fall and 2004 Spring): "security analysis for peer to peer networks"
- Thomas J. Bryant (2004 Spring and Fall): "security analysis for commercial peer to peer networks"
- James Lewis Lyndon (2004 Spring and Fall): "security analysis for commercial peer to peer networks"
- Benjamin K. McCorkle (2004 Spring and Fall): "security analysis for commercial peer to peer networks"
- Joel David Nelson (2004 Spring and Fall): "security analysis for commercial peer to peer networks"
- Negell Monta Ormond (2004 Spring and Fall): "security analysis for commercial peer to peer networks"
- Jonathan Michael Blanton (2004 Fall): "security analysis for commercial peer to peer networks"
- Pranav Harishankar Mehta (2004 Fall): "security analysis for commercial peer to peer networks"
- Nirav Kamlesh Shah (2004 Fall): "security analysis for commercial peer to peer networks"
- Mark Adrian Welter (2004 Fall): "security analysis for commercial peer to peer networks"
- Wassim A Zeitoouni (2004 Fall): "security analysis for commercial peer to peer networks"
- Adam L. McCutcheon (2006 Fall and 2007 Spring): web service secuirty.
- Gabriel Tsu : supported by the NSA project: a networked storage service simulation package, November 2002 to May 2003

7.4 Non-Degree Students Supervised (e.g., certificate students) (N/A)

8 Teaching

8.1 Major Accomplishments

I have been active in enhancing the Information Assurance program in UNC Charlotte. I have developed/introduced the following curriculums at UNC Charlotte to enhance the Information Assurance

program (part of these efforts are based on the educational grant received from various sources such as NSF and DoD): ITIS6240/8240 “Software Testing and Quality Assurance”, ITIS3320 “Introduction to Software Testing and Quality Assurance”, ITIS6320/8320 “Cloud Data Storage”, ITIS 6250/8250 “Open Source Security Systems”. These courses helped the IA program to cover a wide spectrum of the information technology knowledge. Some of these courses (e.g., ITIS6320) are the most popular classes and the class quota is normally filled within hours after the registration is open (the waiting list for the class is 50% of the class size for each semester). Specifically, this helped our students to think about information security from cloud aspects. In the early days of our IA program, I leaded the effort to compile a comprehensive list of topics that each IA course should cover and revised the catalog abstracts of most IA related courses. The reason for revising these curriculums is that: These courses were developed over a period of many years and there are many overlaps among these courses.

As the SIS Graduate Coordinator, I leaded the effort to re-certify the Information Technology Certificate program. As the PhD coordinator for SIS track, I leaded the effort to revise the new qualifying exams process/course requirements for the SIS track PhD students.

I helped Prof. Steve Providence from NC A&T to develop an undergraduate security course at NC AT. This is important for the collaboration between UNC Charlotte and NC A&T program to extend the IA education to under-represented communities.

8.2 Courses Taught

8.2.1 Graduate Courses

- ITIS 6320/8320 Cloud Data Storage (Fall 2017,Spring 2017,Fall 2016, Spring 2016, Fall 2015, Fall 2013). Average students: 35. **This is a new course that I developed.**
- ITIS 6240/8240 Applied Cryptography (Fall 2017,Fall 2016, Fall 2015, Spring 2014, Spring 2012, Spring 2011, Spring 2007, Spring 2006). Average students: 10
- ITIS 6200/8200 Principles of Information Security and Privacy (Fall 2009, Spring 2009, Fall 2008, Fall 2007): Average students: 32
- IT IS 6167/8167: Network Security. (Fall 2005, Fall 2002): average student 30.
- ITIS 6140/8140: Software Testing and Quality Assurance (Fall 2006, Spring 2005, Spring 2004): average student 20. **This is a new course that I developed**.

8.2.2 Undergraduate Courses

- ITIS 3200 Introduction to Information Security (Summer I 2016, Fall 2012, Fall 2011, Fall 2010, Spring 2008, Spring 2007, Spring 2005, Fall 2004, Spring 2004, Fall 2003, Spring 2003): average students 35
- ITIS 3320 Introduction to Software Testing and Quality Assurance (Fall 2013, Spring 2013, Spring 2012, Spring 2010, Fall 2009, Fall 2007, Spring 2006): average student s 30. **This is a new course that I developed**.
- ITCS 2215 Design & Analysis Algorithms (Spring 2011): average student 25

8.2.3 Other Courses (N/A)

9 Service and Outreach

9.1 Accomplishments

The following is a high level summary of my major accomplishments in academic and administrative service (details are included in subsequent sections):

- Leadership roles in major information security conferences: I have been frequently involved in major information security conferences as program committee members
- Leadership roles in the UNC Charlotte annual Cybersecurity symposiums: I was the program committee chair for the 11th cyber security symposium (2010) and was the panel moderators for two years. These activities helped UNC Charlotte's information security outreach effort.
- I have been frequently invited to give talks at institutes and government agencies across the world (e.g., Qatar Ministry of Interior). This helps to enhance the exposure of the UNC Charlotte's information security program.
- I have frequently served on funding agency panels across the world (e.g., USA NSF). This helps to enhance the exposure of UNC Charlotte's information security program.
- As a graduate coordinator, I leaded the effort to re-certify SIS IT certificate program.
- As a PhD track coordinator, I leaded the effort to specify SIS track PhD qualifying exam requirements.

9.2 External Service

9.2.1 Invited Talks

- **Yongge Wang**. From science to engineering: a cryptographic example. Invited talk at Qatar University. November 17, 2014.
- **Yongge Wang**. Introduction to cryptography and building trusted systems from untrusted components. Invited talk at Ministry of Interior (MOI), Qatar. December 30, 2014.
- **Yongge Wang**. Theoretical foundations for cyber security. Invited speaker at "A Roadmap of Research in Cybersecurity: An interdisciplinary perspective" sponsored by The British Embassy (Doha), The British Council, Open University, and Qatar University. March 15, 2015.
- **Yongge Wang**. Cybersecurity Challenges For Smart Grid Systems: From Cryptographic Viewpoints. Invited distinguished speaker at "First workshop on Smart Grid and Renewable Energy, SGRE 2015", Doha, Qatar, March 23, 2015
- **Yongge Wang**. Statistical Testing for pseudorandom generators. Invited talk at Nankai Institute of Mathematics (In memory of Prof. Hu's 90 Birthday). May 2013
- **Yongge Wang**. Statistical Testing for pseudorandom generators, array BP-XOR codes etc. Invited talk at Hexi University. June 2013
- **Yongge Wang**. I was invited by "5th Conference on Logic, Computability and Randomness, 2010, May 24 - 28, University of Notre Dame, South Bend, IN, USA." To give an invited talk on the "Survey of 10 years' achievement on effective randomness research". This conference was sponsored by NSF and all the conference and travel cost were paid by NSF.
- **Yongge Wang**. Design Cryptographic Techniques That Could Be Directly Used by Industry. Invited Lecture at Guangdong Key Laboratory of Information Security Technology (Sun Yat-sen University, June 12, 2007) http://ist.sysu.edu.cn/ShowScience.asp?id=4
- **Y. Wang** is the invited speaker at Shanghai University of Electric Power (June 13, 2005) http://www.shiep.edu.cn/news/show.asp?id=1654
- Invited Panel co-moderator of 2005 Annual Security Symposium at UNC Charlotte
- Invited Panel co-moderator of 2006 Annual Security Symposium at UNC Charlotte

9.2.2 Journal/Conference Reviewer

- Regular reviewer for AMS Mathematics Review, and referees for many journals and conferences: IEEE Transactions on Information Theory, IEEE Transactions on Information Forensics & Security, IEEE Communications Letters, Journal Information Processing Letters, Journal Cryptography and Communications, Conference ICALP, IEEE ICDM Conference, Crypto conference, Eurocrypt conference, Information Processing Letters, IBM Journal on Systems, Journal of Computer Security, Theoretical Computer Science, IEEE Transactions on Wireless Communications, IEEE Transactions on Dependable and Secure Computing, The Computer Journal, Journal of Computer Science and Technology, and many others
- IEEE 1363 Standards Voting Member since 2006.

9.2.3 Program Committees (PC)

- PC Member of annual IACR workshop on Public Key Cryptography Conference (PKC) 2003
- PC Member of the 4th International Conference on Cryptology and Network Security (CANS) 2005.
- PC Member of annual International Conference on Security and Cryptography SECRYPT 2006
- PC Member of annual International Conference on Security and Cryptography SECRYPT 2007
- Program Committee Chair of the 11th UNC Charlotte Annual Security Symposium 2010
- PC Member of annual Information Security Conference 2013

9.2.4 Editorial Boards/Panels

- Panel member for Kentucky Science & Engineering Foundation (two times: 2006 and 2007). http://ksef.kstc.com. Project manager is: Liz Knapp (200 West Vine Street, Suite 420, Lexington, KY 40507, phone: (859)255-3613 x245 fax: (859)259-0986, email: lknapp@kstc.com)
- Panel member for Canada MITACS research funding (2007)
- Panel co-moderator of Annual Security Symposium at UNC Charlotte (2005 and 2006)
- Panel member for Austrian Science Fund (2015)
- Panel member for USA NSF research funding (four times: 2009, 2010, 2013, 2016, 2017)
- I was invited to evaluate the cryptographic techniques that have been submitted to Japanese government standard committee IPA. The cryptographic techniques standardized by IPA has become the Japanese government standards

9.2.5 Professional Affiliations/Memberships

- Member of AMS (American Mathematical Society)
- Member of ACM
- Member of IEEE

9.2.6 Community Service

- DH-CHAP was originally proposed for standardization in IETF iSCSI working group. Due to my analysis and attacks, it was finally dropped from the standards. My post and follow-ups could be found http://www.pdl.cmu.edu/mailinglists/ips/mail/msg09610.html
- Cisco and AGA (American Gas Association) had been working on SCADA communication security protocols for several years. When CISCO representative (Dr. Andrew Wright) presented the protocol design (hardware for the protocol had been manufactured at that time) at UNC Charlotte. I broke the protocol within a few hours. Cisco and AGA had to re-design the protocol.
- My research has resulted in several intellectual properties transferred to the UNCC spin-off company Calyptix Corp. I was a co-founder of Calyptix and my share to Calyptix is 5%.
- I helped to start-up the company USMobile and I am currently serving as CSO for USMobile.
- Active participation in the AGA/CISCO/GTI SCADA security standards discussion.
- Active participation in the IETF security standards committees.
- Active participation in the IEEE 1363 standards committees.

9.3 Internal Service

9.3.1 University Committees

- SIS representative to the University Library during (2003-2004)
- The Judge of Niner Across the disciplines: Graduate research competition committee. April 9th, 2005
- Alternative representative for the University Faculty Council (2007-2008)
- University CID/API committee member (2007-2008)
- University Hearing Committee (2012-2015)

9.3.2 College Committees

- CCI graduate committee member (2002-2003)

- CCI Lab Equipment committee member (2004-2005)
- CCI undergraduate committee member (2006-2007)
- CRC member (2008-2009)
- One time teaching award committee member (2009-2010)
- Friday research seminar coordinator (2009-2010)
- Secretary for CCI Faculty meeting (2011-2012)

9.3.3 Department Committees

- PhD steering committee (2004-2005, 2007-2008, 2009-2010, 2015-2018)
- Chair of the SIS faculty search committee (2004-2005)
- SIS faculty search committee member (2005-2006)
- Chair of graduate committee (2007-2008)
- Graduate committee member (2008-2009, 2011-2012 and 2012-2013)
- Chair of Department Review Committee (DRC) (2009-2010, 2017-2018)
- Undergraduate Committee member (2009-2010)
- Department Review Committee (DRC) member (2010-2011)
- Faculty research committee member (2013-2014)
- PhD coordinator (2015-2017)

9.3.4 Ph.D. Dissertation/Master's Thesis/Baccalaureate (Honors) Committees

- PhD committee chair for the following students: Libin Bai, Lida Safarnejad, and Eduardo Eckmann
- PhD committee member of Lawreance Teo (SIS), Yonggang Wang (Math Department), and Meijiao Zhang (Math Department).

9.4 Other Service (N/A)

10 Leadership

I have played leadership roles in research, teaching, and service during last decades. The following is a summary of the impact of several leadership efforts:

- As the Chair of SIS faculty search committee (2004-2005), I leaded the effort for advertising, screening, and interviewing candidates to develop an HCI program at UNC Charlotte. Before 2005, SIS Department had no HCI faculty. The search committee had done a very good job and hired the first HCI faculty during that year. After that, we have developed a strong HCI group in UNC Charlotte.
- As the Graduate Coordinator for SIS department (2008-2009), I leaded the effort to revise all certificate programs. Specifically, I leaded the effort to re-organize the curriculums for certificate programs and leaded the effort to re-certify the IT management certificate program. This helped to align our certificate programs with the development of new technology in IT industry.
- As the Chair of SIS Department Review Committee (DRC 2009-2010), I leaded the effort to revise SIS promotion and tenure policy. The effort is to emphasize the leadership roles for promotion to full professorship. The impact is to motivate SIS faculty to establish leadership roles in research, education, and service.
- As the Program Committee Chair of the 11th UNC Charlotte CCI Annual Security Symposium (2010), I managed to run a very successful symposium. I also helped to establish the system for obtaining CISSP credits for symposium attendees. This helped to attract more attendees to the security symposium and helped CCI to actively outreach the local community.
- As the Lead PI, I organized a high profile international team of researchers to secure US$810,000 research fund from Qatar Foundation in 2015. The Qatar Foundation funding rate for 2015 is 14% and is very competitive. The team includes world top researchers: Prof. Yvo Desmedt (UT Dallas), Prof.

Prof. Qutaibah M. Malluhi (Qatar University), and Prof. Yuliang Zheng (University of Alabama). This project will help establish UNC Charlotte's leadership roles in efficient coding technique development for cloud storage systems.

- I played the leadership roles in the international algorithmic information theory research. My research findings have become the basic theorems in this research direction and mathematicians from top universities are doing research based on my results (these follow-up researches could be found here: http://scholar.google.com/scholar?oi=bibs&hl=en&cites=7764890318265415 00,270438365819495471,4993792158199359388 and http://scholar.google.com/scholar?oi=bibs&hl=en&cites=8951704309235383187).
- I played the leadership roles in cryptographic technology transfer from research to industry. I invented/designed remote password authentication protocols, identity based key agreement protocols, XML security protocols, and SCADA security protocols. These protocols have been standardized by the major industry standards bodies such as IEEE, AGA, W3C, and IETF. They have been widely deployed in industry. For example, the XMLENC/XMLDsig security protocols are used in almost all XML related products in the world. Currently, I am participating in the NIST standards effort for post quantum cryptography (http://csrc.nist.gov/publications/drafts/nistir-8105/nistir_8105_draft.pdf) and hope to include my post-quantum encryption protocol RLCE in the final NIST standards.
- I have leaded the effort to develop several major courses (new courses) to enhance UNC Charlotte's Information Assurance Program. These courses include (but not limited to): cryptography, cloud data storage, open source software security, and software testing and assurance.

11 Research Statement

I received my bachelor/master degree in pure mathematics and PhD degree in theoretical computer science. I worked as post-docs in information security domain for a few years. Then I joined industry for a few years until I returned to academics in 2002. This interesting career path from pure theory to practical products shaped my research philosophy. My research achievements have reflected this philosophy which will be described in the following.

Theory: I have worked in several areas of theoretical research such as mathematical logic (recursion theory, model theory), algorithms and computational complexity, probability theory, randomness, and pseudo-randomness. One of the most influential and important results in my PhD thesis is a theory that helps to understand what the randomness it is. Since Kolmogorov (also Einstein's Brownian motions theory), mathematicians, physicist, and information theory scientists have tried to understand what a good definition for randomness is. I proved a very beautiful theorem which gives a perfect solution. That is, an infinite sequence is random if and only if it is the sum of the probability of a universal Turing machine halting problem. Combining Einstein's characterization of Brownian motions, we can interpret this theory as: you know when your computer crashes if and only if you know what the next movement of a particle in the liquid is. This result initiated a new research direction and many mathematicians in top universities have been working in this new area for last decades (it is still a very active research area though I am no long working in that area).

Randomness in practice: Pseudorandom generators are the fundamental components of cyber security. For example, e-commerce web services use TLS/SSL to establish secure connections between the client computers and server computers. If the random generators of the web servers were not strong enough, a hacker could easily break into these connections to eavesdrop on these "secured" connections and to impersonate the e-commerce web service to clients. Then one may ask: is that possible to test whether a web server's randomness generator is secure or not before deployment? The answer is that no existing technique could do this. Although there are state-of-the-art pseudorandom testing techniques such as US government NIST SP800-22 standard, I have carried out extensive experiments (based on over 200TB of random bits generated). The experiments show that NIST SP800-22 techniques could not detect several widely deployed well-known weaknesses in pseudorandom generators for e-commerce web services. The experiments further

show that NIST SP800-22 even could not detect the well-known weakness in the Debian's OpenSSL release CVE-2008-0166's pseudorandom generators. Based on these motivations, I designed statistical distance based LIL testing techniques (analogy of Einstein's Brownian motion theory). My experiments show that my new techniques could easily detect the above mentioned weaknesses in web service pseudorandom generators. The software package for my testing techniques is available on my webpages for non-commercial purposes.

Secure communications: I have done extensive research in the areas of secure communication for several scenarios such as:

- Some parties in the system are not trusted and no public key technique is used,
- Remote password authentication is needed with robustness against offline dictionary attacks, and
- Identity based remote authentication is needed.

My research results have been published in tier-1 flagship venues such as IEEE Transaction on Information Theory, Crpyto, Eurocrypt, Journal of Cryptology, and ESORICS. These results have extensive industry impact.

Infrastructure security (Cyber Physical Security CPS): I have done extensive research in control system security and controller/smart meter security. Some of my results have large impact on national critical infrastructure protection and I frequently speak on venues for smart grid system security. For example, I have broken the SCADA security techniques designed by Cisco researchers for American Gas Association (AGA) and helped AGA/CISCO to design a secure SCADA solution. These designs have been adopted as a part of IEEE 1711 standard which is used to protect the national SCADA control system security. I have also designed several authentication protocols for protecting tamper resistant device (controller/smart meter) widely deployed for the renewable energy and smart grid systems.

Coding theory and post-quantum cryptography: I am the inventor of array BP-XOR codes which is based on ideas from digital fountain and LDPC codes. These codes have been used in privacy preserving cloud data storage and also in cloud and big data storage. I also do research on post-quantum cryptographic techniques and have designed coding based public key encryption scheme RLCE (Random Linear Code based Encryption).

12 Teaching Statement

My teaching philosophy is to provide students with a global picture of the entire field. For example, in network security courses, there are numerous standards for students to learn and it is hard for them to understand. I provide students with a clear intuition and motivation behind each step in the protocols and standards. This proves to be very successful in my class. I also encourage student's participation in all parts of my class. For example, in my class, students may grade their peer's programming-based projects (as double-blind review). At the end of the projects, students suggest their preferred designs and types of new projects. I take these feedbacks and redesign/improve the projects. I will continue this experiment in other areas such as course material development. I also use extensive hand-on projects to help students understand the concept. For example, during the buffer overflow lecture, some special programs (with buffer overflow issues) are given to students and students are required to modify it with buffer overflow techniques. The more advantage the student gets from the buffer overflow, the more grades they will receive. Another example is that during the firewall and SSL lectures, extensive list of firewalls and SSL products are given to students. Students need to evaluate the advantages and disadvantages of each product and compare their functionality in the end. This gives the chance for students to further understand the concepts underlying these products.

Supervising senior students and graduate students in research is a crucial aspect of my teaching activity. For senior students, it is normally their first experience to do research. Thus they need more attention. I normally have weekly discussions with senior project students about their process and their plan of next week's

research. I fully participate in student senior projects. For example, I set up a peer to peer network in my office and let students to connect to it. For graduate student research, I give them more freedom. Weekly meeting with students is required by me. During the meeting, students report their progress and their new findings. I help them identify the future directions.

Teaching is important to me for several reasons: it provides excellent opportunity to interact with intelligent students and to learn from them; it enables me to expose my research to students and to get feedback from them; it enables me to achieve better understanding of the research topics; and it provides me the chance to serve the community.