

CURRICULUM VITAE

YONGGE WANG

ADDRESS AND CURRENT POSITION

PhD, CISSP
Assistant Professor
Department of Software and Information Systems
University of North Carolina at Charlotte
9201 University City Blvd. Charlotte, NC 28223
Phone: (704) 6875491
Email: yonwang@uncc.edu
Homepage: <http://www.sis.uncc.edu/~yonwang/>

EDUCATION

09/1988–07/1991 M.Sc. Computer science, 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.

ACADEMIC EXPERIENCE

08/2002– now Assistant Professor at University of North Carolina at Charlotte
07/1999–04/2000 Research associate at the CACR of University of Waterloo <http://cacr.math.uwaterloo.ca/>
11/1997–06/1999 University of Wisconsin at Milwaukee. Research associate on a DARPA project called “survivability in the distributed network”. <http://cs.fsu.edu/~desmedt/survivability/>.
01/1997–10/1997 Auckland University (New Zealand). Research associate (in Professor Cristian Calude’s group <http://cs.auckland.ac.nz/~cristian/>)
09/1996–12/1996 Max-Planck-Institute for computer science (Germany). Research associate (in Prof. Herald Ganzinger’s group <http://www.mpi-sb.mpg.de/>)

INDUSTRY EXPERIENCE

05/2000–8/2001 Cryptologic mathematician at **Certicom Corp.** Job descriptions there: 1). Create new patents and analyze Certicom’s patent portfolio. 2). Consultation to the

Product Development in the following standards: IETF IPsec, IETF IPSRA, IETF PKIX, IETF SACRED, IETF TLS, W3C XMLSIG, W3C XMLENC, XKMS, ISO X.509, ANSI X9.series, and WAP protocols. 3). Consultation on the Certicom VPN products. In particular, embedded the Certicom patented MQV key agreement protocol into the IPsec-IKE protocol suite. 4). Consultation to other companies or agents. E.g., one of the principal authors of the evaluation report to Japanese Government IPA project: Evaluation of Security Level of Cryptography Digital Signature Schemes. 5). Participation in standardizing Certicom patented protocols and products. 6). Participation in IETF and W3C standardization process. The author of several requests for comments (RFC) on XML security. 7). Doing independent scientific research and publishing papers.

- 10/2001–07/2002 Senior security specialist at the start-up company Karthika Technologies Inc. Job descriptions there: 1). Designed the comprehensive solution for the Storage Area Networks. 2). Protocol design and presentation to ANSI T11.3 working group. 3). Software design (including coding of all parts of the products) from scratch to productization. Karthika was acquired by a public company: KastenChase Applied Research Labs, in March 2002.
- 02/1999–06/1999 Programmer at Medical College of Wisconsin. Designed the on-line physician and patient web database for all affiliated hospitals of MCW (<http://doctor.mcw.edu/>) (using mySQL and ORACLE). The database can be accessed and updated via browsers (using Perl CGI scripts).

RESEARCH FUNDING

- 01/2003–08/2003 PI (no coPI) of “Strategic Plans for Secure Storage Systems” supported by Bank of America. Amount US\$43,939.
- 09/2003–08/2005 co-PI of “Privacy preserving database application testing” supported by NSF CCR-0310974. Amount US\$200,000.
- 01/2004–06/2004 PI (no coPI) of “Faculty Research Grants” supported by UNC Charlotte. Amount US\$4300.
- 09/2005–02/2006 co-PI of “Honeynet Research and Experience” supported by Bank of America. Amount US\$50,000.
- 01/2006–06/2006 PI (no coPI) of “Faculty Research Grants” supported by UNC Charlotte. Amount US\$6000.

FUNDING FOR EDUCATION PURPOSE

- 01/2005–06/2005 PI (no coPI) of “Curriculum and Instructional Development Grant” supported by UNC Charlotte. Amount US\$5100.
- 09/2002–08/2003 co-PI of “DoD Carolinas Cyber-Defender Scholarship Program” supported by DoD IASP. Amount US\$350,418.

09/2003–08/2004 co-PI of “DoD Carolinas Cyber-Defender Scholarship Program” supported by DoD IASP. Amount US\$201,460.

INVITED AND PEER REVIEWED BOOK CHAPTERS

1. Y. Wang. PKCS: Public-Key Cryptography Standards. In *Handbook of Information Security* (editor: Dr. Bidgoli), John Wiley & Sons, Inc., 2005.
 2. Y. Wang. Securing eBusiness with cryptographic techniques In *Bank Fraud and IT Security* December 2004 Issue, by Southeast Consulting Inc. (Invited but not reviewed article)
-

PEER REVIEWED JOURNAL PUBLICATIONS

1. 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, 7 March 2006.
2. Y. Wang. Robust key establishment in sensor networks. *ACM SIGMOD Record* **33**(1):14–19, March, 2004.
3. 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.
4. Y. Wang. A comparison of two approaches to pseudorandomness. *Theoretical Computer Science* **276**(1-2):449–459, 2002.
5. Y. Wang. The algebraic structure of the isomorphic types of tally polynomial time sets. *Archive for Mathematical Logic* **41**(3): 215–244, 2002.
6. W. Merkle and Y. Wang. Separations by random oracles and almost-classes for generalized reducibilities. *Mathematical Logic Quarterly* **47**(2):249–269, 2001.
7. Y. Wang and Y. Desmedt. Secure communication in multicast channels. *Journal of Cryptology* **14**(2):121–135, 2001.
8. C. Calude, P. Hertling, B. Khoussainov, and Y. Wang. Recursively enumerable reals and Chaitin’s Ω numbers. *Theoretical Computer Science* **255**:125–149, 2001.
9. 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.
10. Y. Wang. Resource bounded randomness and computational complexity. *Theoretical Computer Science* **237**(1-2):33–55, 2000.
11. Y. Wang. Category, measure, and polynomial time approximations. *SIAM Journal on Computing* **28**(2):394–408, 1999.
12. Y. Wang. A separation of two randomness concepts. *Information Processing Letters*, **69**(3):115–118, 1999.
13. Y. Wang. Randomness, stochasticity, and approximations. *Theory of Computing Systems* (formerly: *Mathematical Systems Theory*) **32**:517–529, 1999.

14. Y. Wang. Abuses of probabilistic encryption schemes. *IEE Electronics Letters*, **34**(8):753–754, 1998.
 15. P. Hertling and Y. Wang. Invariance properties of random sequences. *Journal of Universal Computer Science*, **3**(11):1241-1449, 1997.
 16. Y. Wang. NP-hard sets are superterse unless NP is small. *Information Processing Letters* **61**(1):1-6, 1997.
 17. Y. Wang. Modified data-flow models and their applications. *Chinese Journal of Software*, **5**(3):43-48, 1994.
 18. G. Hu and Y. Wang. The fundamental theory for object-oriented languages. *Chinese Journal of Computer Science*, **20**(4):1-6, 1993.
 19. Y. Wang. The computing power of ordered Petri nets. *Chinese Journal of Software*, **4**(3):35-41, 1993.
 20. S. Xu and Y. Wang. Blum's speedup theorem and the hierarchy of recursive functions. *Chinese Journal of Software*, **4**(4):38-43, 1993.
-

PEER REVIEWED CONFERENCE/SYMPOSIUM/WORKSHOP PUBLICATIONS

1. 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.
2. Y. Wang and X. Wu. Approximate inverse frequent itemset mining: privacy, complexity, and approximation. In *Proc. 5th IEEE ICDM* (ratio: 69/630). pages 482-289, 2005.
3. 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.
4. 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.
5. 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.
6. 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.
7. 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)*, Lecture Notes in Computer Science 3488, Pages 382–390, Springer, 2005.
8. 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) Lecture Notes in Computer Science 3184, pages 142-151, 2004, Springer-Verlag.

9. 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.
10. 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.
11. 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.
12. Z. Liu and Y. Wang. A secure agent architecture for sensor networks. In *Proceedings of The 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 (Eds. H.R.Arabnia, R. Joshua, and Y.Mun), CSREA Press.
13. Y. Wang, Y. Zheng, and B. Chu: Efficient and secure storage systems based on peer-to-peer systems. In *Proceedings of The 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 (Eds. H.R.Arabnia, R. Joshua, and Y.Mun) CSREA Press
14. 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
15. Y. Desmedt and Y. Wang. Maximum Flows and Critical Vertices in AND/OR Graphs. In *Proceedings of COCOON '02*, pages 238-248. Lecture Notes in Computer Science 2387, Springer-Verlag. Preliminary results were presented at *INFORM '99 Cincinnati*, section SA34.1.
16. Y. Desmedt and Y. Wang: Perfectly Secure Message Transmission Revisited. In *Proceedings of EuroCrypt'02*, pages 502-517. Lecture Notes in Computer Science 2332, Springer-Verlag.
17. 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.
18. 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.
19. Y. Desmedt and Y. Wang. Approximation hardness and secure communication in broadcast channels. In *Advances in Cryptology, Proc. of Asiacrypt 99*, pages 247-257. Lecture Notes in Computer Science 1716, Springer Verlag.
20. 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.
21. C. Calude, P. Hertling, B. Khossainov, 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.
22. Y. Desmedt, M. Burmester, 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.

23. Y. Wang. Randomness, stochasticity, and approximations. In *Proceedings of RANDOM 97* (Italy), pages 213–225. Lecture Notes in Computer Science 1269, Springer Verlag.
 24. 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.
 25. 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.
 26. 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.
 27. G. Hu and Y. Wang. An algorithm and its data structure from sequential US MMCM to parallel machine. In *Computer Mathematics*, pages 58-65, World Sci. Publishing, River Edge, NJ, 1993 (MR: 94m:68041).
-

PATENTS AND PATENT APPLICATIONS

1. Yongge Wang. Apparatus for securing SCADA communication links. Filing data: 5/10/2004.
 2. Xintao Wu, Yongge Wang, and Yuliang Zheng. Apparatus and methods for privacy preserving database application testing. Filing date: 10/10/2003.
 3. Yongge Wang, Clement Kent, and Daniel Thanos. Authentication protocols for networked storage devices. Canada patent application 2,375,898, Filing date: 03/11/2002.
-

OTHERS: PRESENTATIONS, PUBLICATIONS, AND POSTS

1. 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)*
2. “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>
3. 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>
4. 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
5. 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

6. 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
7. A. Menezes, M. Qu, D. Stinson, and Y. Wang. Evaluation of Security Level of Cryptography: MY-ELLY Signature Scheme. Evaluation report for Japanese government IPA CRYPTREC project. http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1055_elly.pdf
8. 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.
9. 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/maillinglists/ips/mail/msg09610.html>
10. Author 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>
11. "ECDSA with XML DSIG" IETF Request for Comments (RFC) 4050. <http://www.ietf.org/rfc/rfc4050>.
12. Author of ANSI X9.92 draft: Public Key Cryptography For The Financial Services Industry: PV-Digital Signature Scheme Giving Partial Message Recovery

PROFESSIONAL SERVICES

- Member of Program Committee for annual IACR workshop on Public Key Cryptography Conference (PKC) 2003.
- Regular reviewer for AMS Mathematics Review, and referees for many journals and conferences.

PHD THESIS

Y. Wang. Randomness and Complexity. PhD Thesis, 1996.

Main results: Random sequences were first introduced by von Mises in 1919 as a foundation for probability theory. von Mises thought that random sequences were a type of disordered sequences (stochastic approach). Ville constructed a counter example in 1939 to show that von Mises approach is not a good choice. Later, a complete different approach (entropy based) to the definition of random sequences was proposed by Kolmogorov and Chaitin independently, and was further developed by Levin, Schnorr and others. Finally, Martin-Loef (then a student of Kolmogorov) developed a third approach (typicalness based) to the definition of random sequences in 1966. In 1970s, Schnorr tried to give a uniform approach to the definition of random sequences using martingales. Later, Lutz introduced these concepts to the computational complexity theory. A long open question in this area had been the following one: were recursive martingale based random sequences the same as effective non-constructivity based random sequences? van Lambalgen (1987) and Jack Lutz (1992) have conjectured that they are different. Indeed, this problem had been open since Schnorr's work

in 1971. van Lambalgen and Lutz re-examined this problem due to its increasing importance in the complexity theory at that time. Many researchers in this area had tried to solve this problem without success. Using a novel construction, I showed that these two concepts are indeed different in 1995. Chaitin called the halting probability of a universal self-delimiting Turing machine the Ω number. Ω number is the most complicated computable number since it is random. When working with Chaitin in IBM Watson research lab, Solovay defined the concept of Ω -like numbers. Roughly speaking, a real number is Ω -like if its approximation dominates the approximation of all other computable real numbers. Solovay showed that Chaitin's Ω number is Ω -like. We showed that indeed, each Ω -like number is a Ω number. Then we conjectured several possibility for computable real numbers. Professor Slaman from UC Berkeley has answered all these conjectures affirmatively.

STUDENTS

Senior projects	Bradley Michael Reavis, Johnathan Lee Moore, William Christopher Kees, Aman Mayson, Robert Brian Lockwood, Jason Matthew Allen, Michael Brian Dickerson, Roman Pyzh, Dimitre Todorov Stanimirov, Chung K Tran
Master students	Ashish Vijaywargiya (2003, Msc project), Anita Sehgal (2004, Msc thesis), Hariharan Venkatasubramanian (2004, Msc project), Atish Ashokkumar Shah (2004, Msc thesis)