University at Buffalo
State University of New York

Department of Computer Science and Engineering

January 16, 2014

Prof. Reneta Barneva, Chair
Department of Computer and Information Sciences
2148 Fenton Hall
SUNY Fredonia
Fredonia, NY 14063

Dear Professor Barneva:

I am delighted to provide a reference for Dr. Qi Duan, who has applied for your Assistant Professor opening. He defended his PhD dissertation "On Graph Related Protocols and Algorithms in Wireless Security" in August 2009. I have known him since he was originally a student in my department in 1999–2000, and then after his return from an industry job in 2003.

After a one-year position at Geneseo, he obtained a postdoc with Dr. Ehab Al-Shaer of UNC Charlotte. This has proved to be a great opportunity for him, lasting over three years. The DLBP server lists 15 papers for Al-Shaer in 2013 and 12 in 2012; Qi is on 5 of those papers this past year, and 2 from 2012. Qi is first-author jumping out of alphabetical order on three of them, including one in the July 2013 issue of *IEEE Communications*, which is very mainstream. I recognize the use of logic-based structuring and analysis of protocols via ordered binary decision diagrams, since Qi has asked me a couple questions about logic over these years. I don't have any further involvement than this, but my colleague Professor Jinhui Xu has kept up work on difficult graph algorithms, including the acceptance last fall of a joint paper "On the Connectivity Preserving Minimum Cut Problem" to the *Journal of Computer and Systems Sciences*. This work I actually talked about with David Johnson over a lunch at the 2009 FOCS conference, he being about the best person one could ask to verify that they were hitting the correct formulation of an important problem and that their solution is new. (Some other luminaries heard the conversation, including Richard J. Lipton whose popular weblog *Gödel's Lost Letter and P=NP* I have joined as partner.)

Aside from this I can tell you more about our history and his character as a researcher. He started with interest in algebraic aspects of computational complexity theory, which is in my specialty, but after 2003 he turned his algebraic knowledge toward cryptographic and network protocols, working with my colleague Professor Shambhu Upadhyaya and students in his group. I was ill myself for two years with symptoms evidently due to over-prescription of the drug Reglan, and part result is that I did not follow him into this work—we have no joint papers. However, I guided Qi through his proposal and thesis writing, converted him from Word to LaTeX, and helped with algorithms and complexity questions that arose. He also served excellently as a TA in some of my theory courses.

Qi worked in closest partnership with Upadhyaya's senior students Mohit Virendra and Murtuza Jadliwala, who also defended their dissertations the same summer. Their papers were successful, e.g. one was accepted to the 2009 ACM Conference on Wireless Network Security in Zurich, which per http://www.sigsac.org/wisec/WiSec2009/accepted.html had fewer accepted papers (28) than members of the program committee (32). I'll reiterate things I said when writing for him then, despite the years-ago dates, so as to portray the range anchored by his work under Al-Shaer. The main theory in that 2009 paper was by first-author Murtuza, but some of the content built on chapter 4 of Qi's dissertation—and the three students scrupulously segregated all material in their

Davis Hall Room 338, Box 602000, Buffalo, NY 14260-2000
Tel: (716) 645-3180 Fax: (716) 645-3464

dissertations rather than pad with overlaps. Qi had the lead role in his paper "Server Based PMK Generation With Identity Protection For Wireless Networks" with Virendra presented at the 4th Workshop on Secure Network Protocols (NPsec'08) alongside the major ICNP'08 conference (see `http://www.netsec.colostate.edu/npsec08/program.html` for program). This is based on a chapter that Qi *removed* from his dissertation, since it wasn't related to graphs, algorithms, or complexity.

An earlier paper on minimum-cost network-blocking problems appeared in the proceedings of the 2007 IEEE International Conference on Communications (ICC'07), while another on graph-theoretic problems was invited to a journal special issue and appeared. The network algorithms and complexity hardness results in these papers are primarily by Qi, who was meaningfully first-author on the ICC'07 paper (that's how Shambhu's group does it, while the theory community tends to go alphabetical). Their paper "Detecting Cheating Aggregators and Report Dropping Attacks in Wireless Sensor Networks" (Virendra-Duan-Upadhyaya) won second prize out of twelve full-length presentations in an all-day overview of departmental research run by the UB CSE graduate students in March 2008.

The conclusion from all of this is that Qi's work has jelled nicely, and he can do strong research in a number of different areas: graph-theoretic network models, algorithms for network problems, theoretical limitations of such algorithms, interconnection networks for large-scale distributed systems, and protocols for trustworthy computation in distributed systems. He is adept in logic and the lengthy use of formal methods. Overall, sensor networks and security are a major strength of our department in which several others of our theory/algorithms faculty participated, and Qi has demonstrated long-lasting benefit from the synthesis of theoretical and practical content. He would be perfect for a research group with a similar spread of interests—looking at your faculty page, he would fit with Profs. Tsetse and Zubairi while giving you more on the protocol and security side.

He showed skill both at solving problems and in developing new concepts, and his analysis is exceptionally accurate (as also his grading was as my TA). He is also good at self-criticism, not getting "carried away" by his ideas, and works hard—indeed he could have been more voluble in telling me all his current work, but mentioned instead a difficult issue he was grappling with. His personal comportment has been exemplary, both as a TA (in mine and others' courses) and as a research student. In sum I can recommend him most highly, and I will be happy to answer any further questions you may have.

Yours sincerely

Dr. Kenneth W. Regan
(716) 645-4738, `regan@buffalo.edu`