University at Buffalo
State University of New York

Department of Computer Science and Engineering

September 25, 2015

Prof. Robert Beverly
Computer Science Department
The Naval Postgraduate School
1 University Circle
Monterey, CA 93943

Dear Prof. Beverly:

I am delighted to provide a reference for Dr. Qi Duan, who has applied for your Assistant Professor openings on the strengths of his record in both computer security and data science. He defended his PhD dissertation "On Graph Related Protocols and Algorithms in Wireless Security" in August 2008. 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 proved to be a great opportunity for him, lasting over three years. Indeed Qi is on 6 of Al-Shaer's papers from 2013 according to the DBLP server and 2 each from 2014 and 2015 so far; Qi is first-author jumping out of alphabetical order on 4 of them, including one in the July 2013 issue of *IEEE Communications*, which is very mainstream.[1] Qi contacted me about the use of logic-based structuring and analysis of protocols via ordered binary decision diagrams in several of them, so I recognize that as a special part of his contribution. I don't have any further involvement than this, but my colleague Professor Jinhui Xu has kept up work on difficult graph algorithms. This includes the joint paper "On the Connectivity Preserving Minimum Cut Problem" in the *Journal of Computer and Systems Sciences*. This work began while Qi was still writing his dissertation officially under my direction but also in large part by Jinhui and another colleague, Shambhu Upadhyaya; a fruitful talk I had with David S. Johnson clarified to me that Qi and Jinhui were hitting the correct formulation of an important problem and that their intended solution would be new. The final paper has incredibly difficult graph-theoretic constructions and also weighs in on the relation of problems in NP to "quasi"-polynomial time.

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 turned his algebraic knowledge toward cryptographic and network protocols, which is Upadhyaya's area. I was ill myself for two years 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.

[1] I should mention also that the DBLP entry for Qi lists two papers in 2014–15, both on surface modeling, that are by a different Qi Duan in China.

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

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` (still a valid link) had fewer accepted papers (28) than members of the program committee (32). This has continued through a full journal paper in the *IEEE Transactions on Computers* in 2014, in which the network algorithms and complexity hardness results are primarily by Qi. I'll reiterate things I said in my letters for his position with Al-Shaer in order to portray the range of Qi's expertise: 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 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. This is based on a chapter that Qi *removed* from his dissertation, since it wasn't related to graphs, algorithms, or complexity. I perceive echoes of it in his papers with Al-Shaer and Jafarian on random address, route, and host mutation defenses.

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. Sensor networks, secure data management, and secure protocols have always been a major strength of our department (in fact we recently attracted an expert in differential data privacy), and Qi derived long-lasting benefit from the synthesis of theoretical and practical content. I see that your department has several faculty with a similar combination.

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—indeed he could have been more voluble in telling me all his current work, but mentioned instead a difficult issue he was grappling with. I've always written that he is a hard worker, and recent years have continued to prove it. His personal comportment was 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`