Gaertner *et al.* Reply: As Gao *et al.* point out in the preceding Comment [1], the quantum protocol for detectable Byzantine agreement described in [2] requires an extension to defeat an intercept-resend attack.

In [2], step (iii) stated: ''*C* randomly chooses a position from his list and asks *A* and *B* to inform him about their results on the same position. If all parties have measured in the same basis, their results must be suitably correlated.'' The simple extension of the protocol can be summarized as follows: ''If the parties have measured in different bases, their results must also be correlated according to the predictions of quantum mechanics.'' This allows us to test against the attacks proposed in [1]. A more detailed discussion can be found in [3].

Sascha Gaertner,[1,2,*] Mohamed Bourennane,[3] Christian Kurtsiefer,[4] Adán Cabello,[5,†] and Harald Weinfurter[1,2]
[1]Max-Planck-Institut für Quantenoptik
D-85748 Garching, Germany
[2]Fakultät für Physik
Ludwig-Maximilians-Universität
D-80799 München, Germany
[3]Department of Physics
Stockholm University
SE-10691 Stockholm, Sweden
[4]Department of Physics
National University of Singapore
117542 Singapore, Singapore
[5]Departamento de Física Aplicada II
Universidad de Sevilla
E-41012 Sevilla, Spain

Received 27 October 2008; published 13 November 2008
DOI: 10.1103/PhysRevLett.101.208902
PACS numbers: 03.67.Hk, 03.67.Pp, 42.50.Dv

*ssg@mpq.mpg.de
†adan@us.es

[1] F. Gao, F.-Z. Guo, Q.-Y. Wen, and F.-C. Zhu, preceding Comment, Phys. Rev. Lett. **101**, 208901 (2008).
[2] S. Gaertner, M. Bourennane, C. Kurtsiefer, A. Cabello, and H. Weinfurter, Phys. Rev. Lett. **100**, 070504 (2008).
[3] S. Gaertner, M. Bourennane, C. Kurtsiefer, A. Cabello, and H. Weinfurter, arXiv:0810.3832.

