Schmid *et al.* Reply: In the preceding Comment [1], He proposes an eavesdropping strategy on the single-qubit N-party secret sharing protocol described and experimentally demonstrated in Ref. [2]. As we shall argue, the strategy allows the cheater or cheaters to gain only a small part of the secret and can be fended off completely by a trivial, but appealing, modification of the classical communication part of the secret sharing protocol. This modification makes the protocol simpler than the original one.

According to the protocol of Ref. [2], a single qubit is sequentially transmitted from partner R_1 to partner R_2, and so on until it reaches partner R_N. Each of the N partners is acting on it with a unitary phase operator, where the phase is randomly chosen out of four possible values. Depending on the chosen phase value, the action of each party is divided into classes X or Y (the distinction between the classes is that the two states produced by the actions of type Y are complementary, or unbiased, with respect to the pair of states produced by the X class actions). Only the classes have to be publicly announced after each run in order to determine if the protocol leads correctly to a secret shared bit. In our published Letter [2], these announcements were suggested to be done in a random order.

The strategy presented by He distinguishes two cases, which can occur during the cheating procedure. Suppose the kth partner R_k is cheating. Assume that he/she is asked to reveal the class of action, while not all R_j $(j < k)$ have broadcasted the class of their actions yet. In such an instance, the cheater following He's proposal will not gain any information but will not be caught either. However, there must be, from time to time, instances when the classes of actions from all R_j $(j < k)$ are known to R_k, before he/she is asked to reveal his/her one. In such an instance, the cheater indeed gains an advantage in the sense that a subgroup of $N' < N - 1$ partners, including the cheater, can infer the secret bit value. One must stress that the occurrence of such instances is quite rare and depends, in general, on the actual position of the cheater in the communication chain [they occur with the probability of $(k-1)!/k! = 1/k$]. Thus, the strategy does not allow an effective cheating, especially if one additionally demands that the final secret string is a hash function of the original string of the protocol.

However, there exists a simple solution which ensures that the second case can never occur and, consequently, makes the cheating totally futile. If the broadcasting of the information on the classes of action is allowed only in the reversed order with respect to the order of the qubit transmission, the second, cheating prone, case of He's strategy never happens. For example, in the case of the experimental demonstration from Ref. [2] involving six partners, the qubit is transmitted in the following way: $R_1 \rightarrow R_2 \rightarrow R_3 \rightarrow R_4 \rightarrow R_5 \rightarrow R_6$. According to the present solution, the class choice would have to be revealed by the partners only in the following order: $R_6 \rightarrow R_5 \rightarrow R_4 \rightarrow R_3 \rightarrow R_2 \rightarrow R_1$. The cheater R_k, when asked to reveal his/her class, would never ever know *any* classes of action of R_j with $(j < k)$, which are essentially necessary to gain information on the shared bit when he/she follows He's proposal.

We are very happy that the public discussion with He has led to a further simplification of our protocol. The work is supported by VI Framework EU Programs SECOQC and QAP (Qubit Applications), Deutsche Forschungsgemeinschaft, and Swedish Research Council (Vetenskapsrådet). M. Z. is supported by Wenner-Gren Foundation and MSWiN Grant No. 1 P03B 04927. The collaboration is part of a MNiI/DAAD program.

Christian Schmid,[1,2] Pavel Trojek,[1,2]
Mohamed Bourennane,[3] Christian Kurtsiefer,[5]
Marek Żukowski,[4,3] and Harald Weinfurter[1,2]
[1]Sektion Physik
Ludwig-Maximilians-Universität
D-80797 München, Germany
[2]Max-Planck-Institut für Quantenoptik
D-85748 Garching, Germany
[3]Physics Department
Stockholm University
SE-10691 Stockholm, Sweden
[4]Instytut Fizyki Teoretycznej i Astrofizyki
Uniwersytet Gdański
PL-80-952 Gdańsk, Poland
[5]Department of Physics
National University of Singapore
Singapore 117 542, Singapore

Received 1 September 2006; published 11 January 2007
DOI: 10.1103/PhysRevLett.98.028902
PACS numbers: 03.67.Hk, 03.67.Dd

[1] Guang Ping He, preceding Comment, Phys. Rev. Lett. **98**, 028901 (2007).

[2] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Żukowski, and H. Weinfurter, Phys. Rev. Lett. **95**, 230505 (2005).

© 2007 The American Physical Society