Goldenberg and Vaidman Reply: Peres [1] claims that our protocol (GV) [2] does not present any novel feature, and it is very similar to the oldest protocol of Bennett and Brassard (BB84) [3]. We completely disagree with this claim and with other points raised in the Comment. The essential novelty of our protocol is that the carrier of information is in a quantum state belonging to a definite set of orthonormal states. Any other protocol, as well as the BB84 scheme, does not have this feature, and, in fact, their security is based on that. Let us quote a recent paper [4], coauthored by Peres, stating that "… cloning can give a faithful replica, while leaving the state of the original intact, only if it is known in advance that the carrier of information is in a quantum state belonging to a definite set of orthonormal states. If this is not the case, the eavesdropper will not be able to construct even an imperfect cloning device, which would give some information on the carrier without modifying it: a device of this sort would violate unitarity. Therefore coding based on nonorthogonal quantum states (which cannot be cloned) gives the possibility to detect any eavesdropping attempt." Thus, the security of BB84 (which uses four states, not all orthogonal) is assured by the "no-cloning" theorem, which is not applicable to our case.

Peres claims that in our method Eve has access only to nonorthogonal states: "The $\rho'_{\pm}$ states, *as seen by Eve*, are not orthogonal. They are *identical*." However, the nonorthogonality (as seen by Eve) in our scheme is not "just as in the BB84 protocol." As Peres admits, in the case of *known* sending times our protocol is not secure, yet his nonorthogonality argument remains the same. The security of our protocol is not based on nonorthogonality, but on causality. As we have proved in our Letter [3], a successful eavesdropping is possible only if some information can reach Bob before it leaves Alice's site—therefore, the protocol is secure.

According to Peres, an important common feature of GV and BB84 is that the information is sent in two consecutive steps: the first step is sending the particle, and the second step is sending the necessary classical information, namely the chosen basis (BB84), or the transmission time (GV). The first conceptual difference between the protocols is that in BB84 the two steps are necessary for sending the information, while in GV the first step is enough. The only purpose of the second step is to assure security against eavesdropping. The second difference is that the first step of our protocol also consists of two stages: sending the first wave packet and sending the second wave packet (the delayed one). Alice does not have to wait until the end of the first step for announcing the sending time. She can do that after the first stage of the first step (i.e., after the first wave packet reaches Bob), thus, "the second step" might end before "the first step." These two stages of the first step, i.e., the fact that the quantum signal consists of two separated parts, is the core of our method, and we do not see its analog in BB84 or any other protocol.

Finally, it seems that Peres has not understood the "relativistic" versions of our protocol. First, it is not true that the storage rings have to be larger than the distance between Alice and Bob. When the communication is based on photons which travel on straight lines, the time delay can be made as small as wanted (it depends on the width of the wave packets and on the accuracy of the clocks). Contrary to Peres' claim (and his Fig. 1), Eve can simultaneously access the two branches of the interferometer most of the time; still the protocol is secure. A similar proof to that given in our Letter [3] shows that a successful eavesdropping leads to superluminal signaling. Second, the protocol proposed by us with two widely separated paths and no time delay is secure. Any attempt to redirect the wave packets toward an inspection center invariably increases the flight time of the photons, and therefore, it is exposed by analyzing the timing. Since the information is encoded in the relative phase between the wavepackets, even more sophisticated eavesdropping methods cannot work, unless they use superluminal particles. The security in this case, as we explicitly stated in our Letter, requires large secure users' sites. Fortunately, "large" can be fairly small since the present technology provides very accurate time measurement. Moreover, this simple protocol is conceptually interesting even if the secure sites are large compared to the distance between the users: also in this case no classical secure protocol exists.

This research was supported in part by the Basic Research Foundation (administered by the Israel Academy of Sciences and Humanities) under Grant No. 614/95 and by the National Science Foundation under Grant No. PHY94-07194.

Lior Goldenberg and Lev Vaidman
School of Physics and Astronomy
Raymond and Beverly Sackler Faculty of Exact Sciences
Tel Aviv University, Tel Aviv 69978, Israel

Received 23 April 1996 [S0031-9007(96)00685-0]
PACS numbers: 03.65.–w, 89.70.+c

[1] A. Peres, preceding Comment, Phys. Rev. Lett. **77**, 3264 (1996).
[2] L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).
[3] C. H. Bennett and G Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
[4] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, Phys. Rev. A **50**, 1047 (1994).

