## Comment on "Pulsed Energy-Time Entangled Twin-Photon Source for Quantum Communication"

The aim of this Comment is to point out that, in principle, the protocol for quantum cryptographic key distribution recently described by Brendel *et al.* [1] is not protected against well-chosen attacks. During these so-called Trojan-horse attacks, the owner of the communication net (Eve) simulates the statistics that would be obtained by the users of the device described in [1] (Alice and Bob) thanks to classical light pulses (Fig. 1). In order to simplify the presentation, we limit ourselves to linearly polarized states and we neglect the effect of all of the phase shifters ($\phi = \delta_a = \delta_b = 0$), but the generalization is straightforward.

We also consider an ideal situation in which all components are assumed to be 100% efficient so that our approach has absolutely nothing to do with the visibility or efficiency loopholes. The polarization controllers (PC) allow us to prepare, at will, the polarizations of the pulses in the horizontally, vertically, or diagonally polarized states. The polarization beam splitters (PBS) send the horizontally (vertically) polarized component of the incoming pulse along the short (long) arm of the interferometer so that when Eve prepares a horizontally (vertically) polarized pulse, and when her polarization flipper (PF) is not activated, the pulse will get twice advanced (delayed), split symmetrically into both detectors, and thus behave as a state of the $\{|\text{short}\rangle, |\text{long}\rangle\}$ basis of [1]. Similarly, when the pulse is prepared in one of the diagonally polarized states and the polarization flipper is activated so that it permutes the horizontally and vertically polarized pulses, its components will get advanced once and delayed once, localize in one detector only, and thus behave as a (medium) state of the complementary basis ($\{|\text{short}\rangle \pm |\text{long}\rangle\}$). By performing such preparations at random and imposing the restriction that when both bases are the same so are the polarizations, Eve simulates the correlations of [1], provided she programs the detectors in such a way that one of them clicks at random when both are excited, and only the excited detector clicks otherwise.

At first sight, our result seems to be paradoxical because Bell's inequalities prove that it is impossible to simulate the nonlocal correlations that exist between entangled quantum systems of the type present in [1] by a local mechanism of the type considered by us. In order to solve this apparent paradox, one must realize that Bell, in the establishment of his famous inequalities implicitly assumed that the particles did not know in advance what would be the basis of detection in which they would be tested [2], a condition that is not fulfilled during our attack. Essentially, our type of attack is made possible because, during the realization of the protocol described in [1], Alice and Bob cannot decide actively in which basis

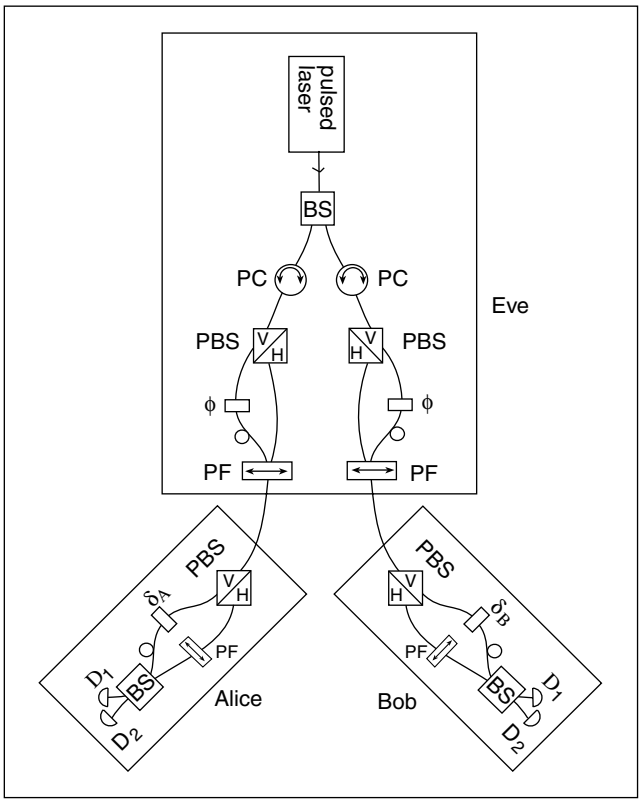


FIG. 1. Eve's device.

the detection will occur. Note that, in virtue of previously established results [3], our approach can be generalized to any situation in which passive elements only are present. It emphasizes the absolute necessity of providing to the users of the cryptographic line the possibility to choose the basis of detection at random, actively, in real time, fast enough, and fully independently.

Support from the Fund for Scientific Research, Flanders, is acknowledged. Sincere thanks to Jason Semitocolos (Clarendon Laboratory, Oxford) for his enlightening presentation of a Trojan-horse attack.

T. Durt
FUND, V.U.B.
Pleinlaan 2
1050, Brussels, Belgium

Received 27 March 2000
DOI: 10.1103/PhysRevLett.86.1392
PACS numbers: 03.67.Hk, 03.65.Bz, 03.67.Dd

[1] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, Phys. Rev. Lett. **82**, 2594 (1999).
[2] L. E. Szabó, Found. Phys. Lett. **8**, 421 (1995).
[3] T. Durt and G. Bana, Found. Phys. **27**, 1355 (1997).

 0031-9007/01/86(7)/1392(1)$15.00 