Quantum Byzantine Agreement with a Single Qutrit

Mohamed Bourennane*
Department of Physics, Stockholm University, SE-10691 Stockholm, Sweden

Adán Cabello†
Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain

Marek Żukowski‡
Institute of Theoretical Physics and Astrophysics,
Uniwersytet Gdański, PL-80-952 Gdańsk, Poland

(Dated: October 30, 2018)

Quantum mechanics provides several methods to generate and securely distribute private lists of numbers suitably correlated to solve the Three Byzantine Generals Problem. So far, these methods are based on three-qutrit singlet states, four-qubit entangled states, and three or two pairwise quantum key distribution channels. Here we show that the problem can be solved using a single qutrit. This scheme presents some advantages over previous schemes, and emphasizes the specific role of qutrits in basic quantum information processing.

PACS numbers: 03.67.Hk, 03.67.-a, 03.67.Dd

It has been recently shown that optimal quantum solutions for some multiparty communication tasks do not require entanglement. Protocols using only the sequential communication of a single qubit have been demonstrated for secret sharing [1] and some communication complexity problems [2]. These protocols were shown to be much more resistant to noise and imperfections than previous protocols based on entanglement. Here we shall present a new example of a problem which can find an optimal quantum solution in the form of a sequential exchange of a single quantum system.

The Three Byzantine Generals Problem (TBGP) expresses abstractly the problem of achieving coordination between the nonfaulty components of a distributed computation when some components fail [3, 4]. Three divisions of the Byzantine army, each commanded by its own general, are besieging an enemy city. The three generals, Alexander, Buonaparte, and Clausevitz (A, B, and C) can communicate with one another by messenger only (i.e., by pairwise authenticated error-free classical channels). They must decide upon a common plan of action: either to attack (0) or to retreat (1). The commanding general A decides on a plan and communicates this plan to the other two generals by sending B a message m_{AB} (either 0 or 1), and by sending C a message m_{AC}. Then, B communicates the plan to C by sending him a message m_{BC}, and C communicates the plan to B by sending him a message m_{CB}. However, one of the generals (including A) might be a traitor, trying to keep the loyal generals from agreeing on a plan. The TBGP is to find a way in which: (i) all loyal generals follow the same plan, and (ii) if A is loyal, then every loyal general follows the plan decided by A.

The TBGP is unsolvable [3, 4], unless the generals share some suitable private data. Each of the generals must be in possession of a list of numbers unknown to the other generals, but suitably correlated with the corresponding lists of the other generals. There is no method, neither classical nor quantum, to guarantee the success of the distribution of the required lists. Nevertheless, a variation of the TBGP, called Detectable Byzantine Agreement (DBA) or Detectable Broadcast [5, 6], which is unsolvable by classical means [7], can be solved using quantum resources [5, 6, 8–12]. In the DBA, conditions (i) and (ii) are relaxed so (i') either all loyal generals follow the same plan or all abort, and (ii') if A is loyal, then either every loyal general follows the plan decided by A or aborts.

Quantum mechanics provides several methods to generate and securely distribute the required lists. So far, these methods are based on three-qutrit singlet states [5, 8, 9], four-qubit entangled states [10, 12], and three [6] or two [11] pairwise quantum key distribution (QKD) channels. In this Letter we introduce a protocol to generate and securely distribute these lists using a single qutrit. We assume that A, B, and C can communicate with one another by pairwise authenticated error-free classical channels and pairwise authenticated quantum channels.

Correlated lists and their use.—The goal of the protocol is to distribute three lists, l_A known only by A, l_B known only by B, and l_C known only by C, all of the same length L, with the property that if 0 (1) is at position j in l_A, then 0 (1) is at position j both in l_B and in l_C, and if 2 is at position j in l_A, then 0 is at position j in one of the other lists and 1 is at position j in the other. The combinations 201 and 210 occur with the same probability [10, 12].

Before we proceed further, note that, on one hand, A knows exactly at which positions the lists l_A and l_B