

I. INTRODUCTION

Entangled states are important for quantum cryptography, being used in several protocols of quantum key distribution. These provide an alternative to single-photon-based protocols. Entangled states are also important in fundamental terms, in the way that the behaviour of these states is contrary to the one predicted by local theories. This contradiction results in the violation of Bell's inequalities, as shown by e.g. the inequality proposed by Clauser, Horne, Shimony and Holt (CHSH).

Entangled states can violate Bell's inequality. However, not all entangled states violate it. Therefore, we say that quantum entanglement is a necessary but not sufficient condition to verify Bell's theorem.

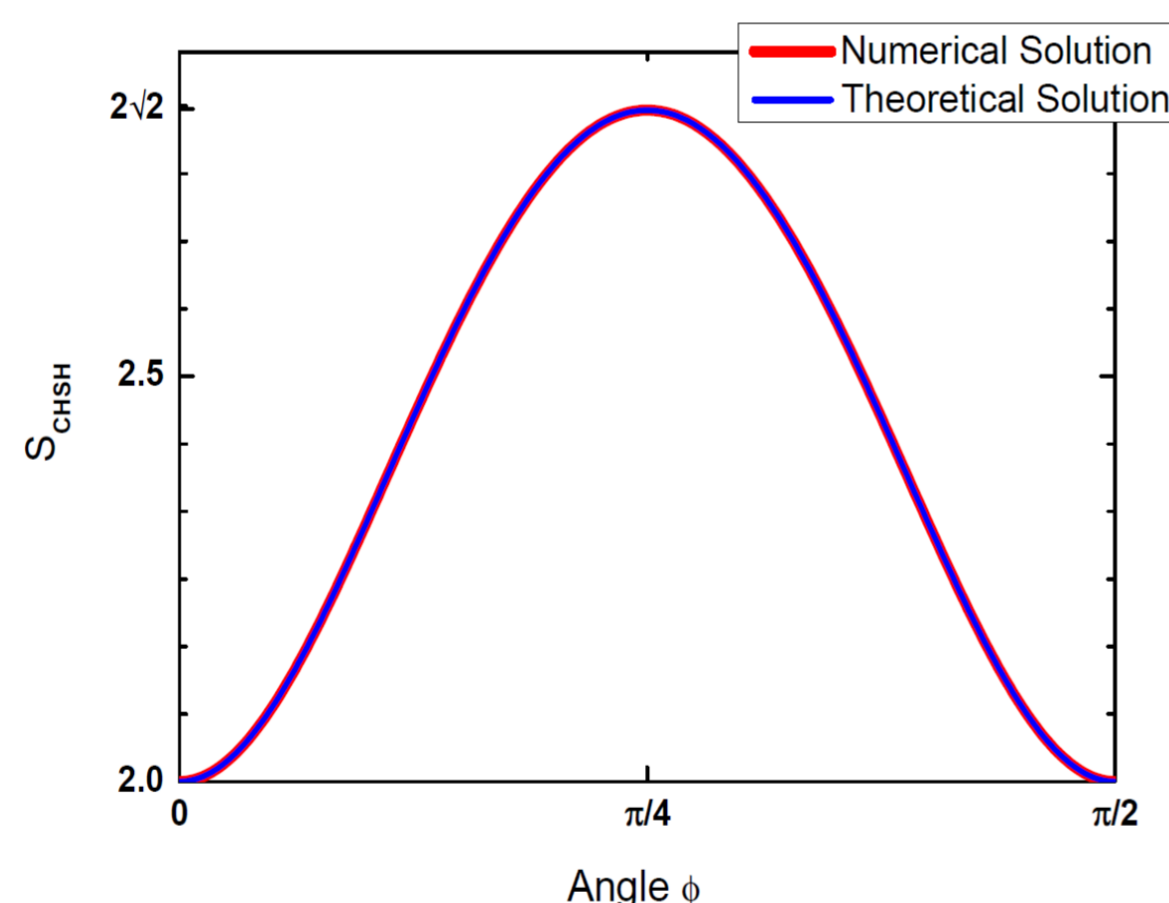
II. QUANTUM STATES AND CHSH INEQUALITY

Entangled states arise when two or more particles are in the same Hilbert space simultaneously, i.e. when it is impossible to factorize its state in individual states. These states are a purely quantum phenomenon, without classical equivalent. For a pair of particles the most convenient way to express Bell's inequality is CHSH's inequality, which has the following form:

$$S = |E(\alpha, \beta) - E(\alpha, \beta') + E(\alpha', \beta) + E(\alpha', \beta')| \leq 2.$$

- **Pure Entangled States:** The classic example of entangled-photon-pair states are the pure states or the so-called Bell states. We also obtained the maximum of violation of Bell's inequality using this state, which has a Shannon entropy of $S = 2\sqrt{2}$.

- **General GHZ States:** The maximum of Shannon entropy is $S = 2\sqrt{\sin^2(2\phi) + 1}$, which is a sufficient condition to verify Bell's theorem. Then, we can say that general GHZ states violate CHSH inequality when $0 < \phi \leq \pi/2$, achieving the maximum when $\phi = \pi/4$, which corresponds to the pure entangled state.



- **General State:** Regarding the general state, we found the maximum of Shannon's entropy, considering a general state of two particles, which has the following form:

$$|\Psi\rangle = a|H\rangle_1|H\rangle_2 + b|H\rangle_1|V\rangle_2 + c|V\rangle_1|H\rangle_2 + d|V\rangle_1|V\rangle_2.$$

- The definition of the maximum Shannon's entropy, which is a sufficient condition to verify Bell's theorem, is closely related to the definition of the correlation function. The maximum of Shannon's entropy is

$$\max(S) = 2\sqrt{A_1^2 + A_2^2 + A_3^2 + A_4^2},$$

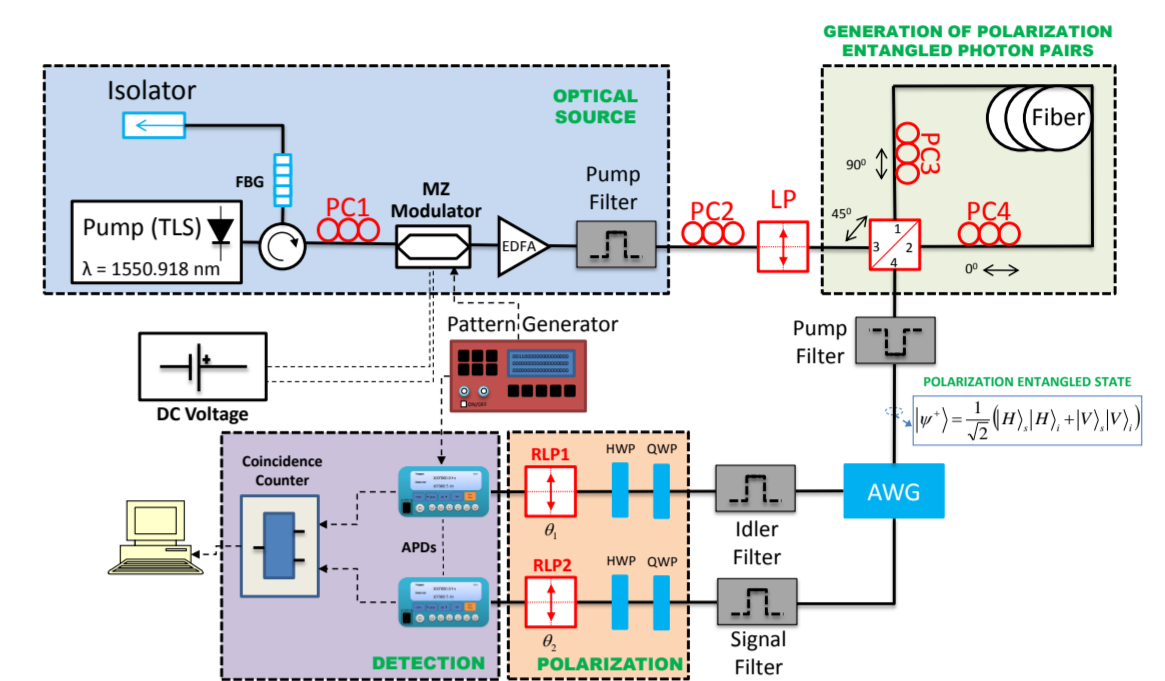
where A_j ($j = 1, 2, 3, 4$) are functions of amplitude eigenstates (a, b, c, d) and have the following expression:

$$\begin{aligned} A_1 &= (|a|^2 - |b|^2 - |c|^2 + |d|^2) \\ A_2 &= (a^\dagger b + ab^\dagger - c^\dagger d - cd^\dagger) \\ A_3 &= (a^\dagger c + ac^\dagger - b^\dagger d - bd^\dagger) \\ A_4 &= (a^\dagger d + ad^\dagger + b^\dagger c + bc^\dagger) \end{aligned}$$

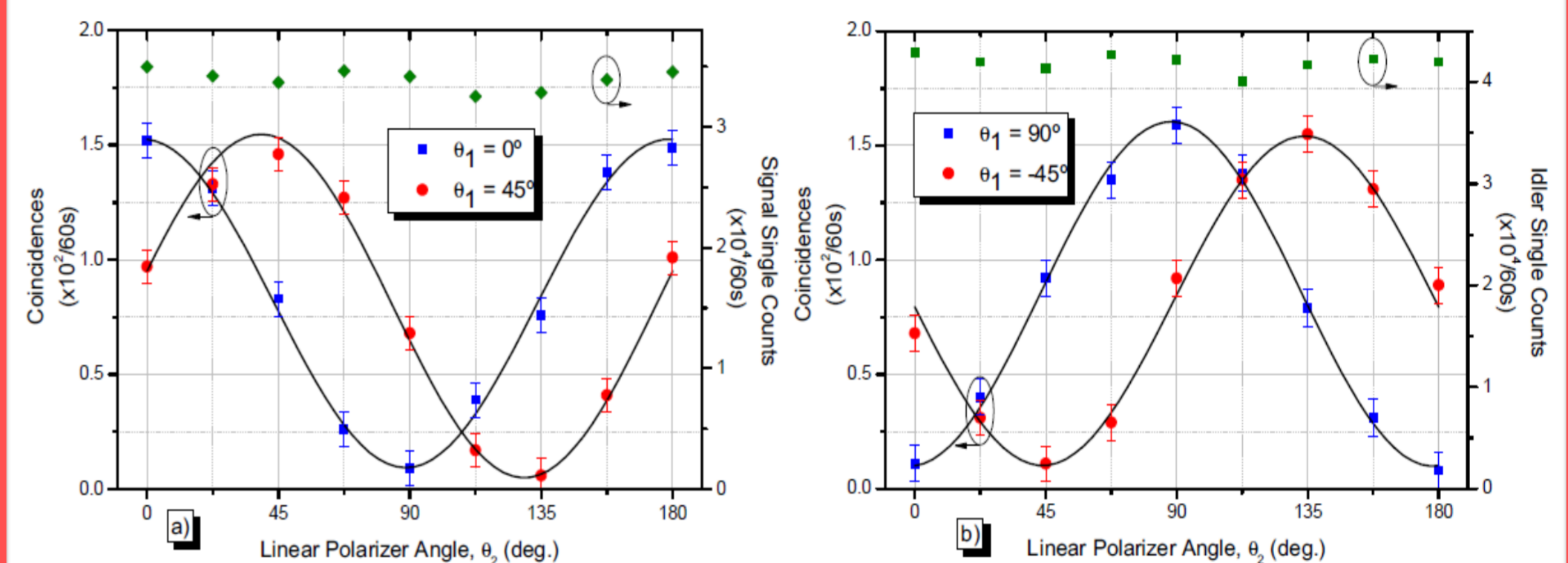
- The relationship between these two quantities gives us clues about a possible general solution of Bell's theorem for states of N -particles.

III. EXPERIMENTAL VERIFICATION

Our experimental setup takes advantage of the spontaneous four-wave mixing process in a highly non-linear fiber to generate the polarization-entangled photon pairs.



Using the experimental configurations determined theoretically for the maximum of Shannon's entropy from the pure entangled state, we obtained the coincidence and single counts shown in the next figure:



The experimental value obtained for Shannon's entropy was $S = 2.47 \pm 0.17$, which is higher than the classical limit of 2. Thus, we verified the violation of CHSH inequality.

IV. CONCLUSIONS

- We addressed comprehensively the fundamental problem of Bell's theorem for systems of two particles.
- We verified theoretically the violation of CHSH inequality not only for the most important states, such as the pure entangled states and the general GHZ states, but also for an arbitrary state.
- From arbitrary states we found a deep relationship between the maximum of Shannon's entropy and the classical correlation function.
- We also verified experimentally the violation of CHSH inequality of pure entangled states.
- The experimental setup used to generate polarization-entangled photon pairs directly into a highly non-linear optical fiber, from the spontaneous four-wave mixing process, have been shown to be suitable for implementation of quantum cryptographic protocols.

ACKNOWLEDGEMENTS

This work was supported in part by the FCT - Fundação para a Ciência e a Tecnologia, through the PhD Grants SFRH/BD/79482/2011 and SFRH/BD/63958/2009, and the Post Doctoral Grant SFRH/BPD/77286/2011 by the FCT and European Union FEDER - Fundo Europeu de Desenvolvimento Regional, through project PTDC/EEA-TEL/103402/2008 (QuantPrivTel), by the FCT and the Instituto de Telecomunicações, under the PEst-OE/EEI/LA0008/2011 program, project 'P-Quantum', and by the Conselho de Reitores das Universidades Portuguesas (CRUP) project 'Ação Integrada E 91/12'.