Erratum: Security of quantum bit-string generation [Phys. Rev. A 70, 052310 (2004)]

Jonathan Barrett* and Serge Massar†

(Received 18 December 2007; published 28 January 2008)

DOI: 10.1103/PhysRevA.77.019904 PACS number(s): 03.67.Dd, 99.10.Cd

The proof of Theorem 1 on page 4 contains an error, and one cannot conclude from the argument given that for classical protocols, the average bias is bounded from below. The mistake is that one cannot commute the max and the summation in the definition Eqs. (3) and (4). This mistake does not affect Theorem 2, which states that no classical protocol is secure with respect to min-entropy, or the analysis of the quantum protocol.

It follows that one cannot conclude that classical protocols must perform badly with respect to the average bias condition. In fact, we learned some time after publishing this article that classical bit-string generation protocols (also called string flipping protocols) do exist, which are secure with respect to the entropy condition and hence also with respect to the bias condition. We refer the interested reader to [1] and references therein. We note that this also has bearing on the interpretation of two subsequent works [2,3] in which experimental realizations of quantum coin tossing and string flipping were reported.

[1] H. Buhrman, M. Christandl, M. Kouck, Z. Lotker, B. Patt-Shamir, and N. Vereshchagink, *High Entropy Random Selection Protocols*, in Proceedings of the 11th International Workshop on Randomization and Computation, August 2007 (RANDOM07); *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, Lecture Notes in Computer Science Volume 4627/2007 (Springer, Berlin, 2007).

[2] G. Molina-Terriza, A. Vaziri, R. Ursin, and A. Zeilinger, Phys. Rev. Lett. **94**, 040501 (2005).

[3] L. P. Lamoureux, E. Brainis, D. Amans, J. Barrett, and S. Massar, Phys. Rev. Lett. **94**, 050503 (2005).

*Present address: Centre for Quantum Computation, DAMTP, University of Cambridge, Cambridge CB3 0WA, United Kingdom. j.barrett@damtp.cam.ac.uk

†Laboratoire d'Information Quantique CP 225, Université Libre de Bruxelles, Boulevard du Triomphe, B-1050 Bruxelles, Belium. smassar@ulb.ac.be

