Errata — Quantum Cryptography and Secret-Key Distillation

Gilles Van Assche

2007-02-22

Introduction

This document lists the known errors in the book *Quantum Cryptography and Secret-Key Distillation* published by Cambridge University Press (2006).

In Chapter 1

- Page 12. In the first sentence of Section 1.1.4, one should read: *For more information, I **would** like to point out* [...].

In Chapter 7

- Page 108. The last sentence of the third bullet should be: *One can easily check that it works provided that $m > l$ and $L > 2l$* (instead of $m > 2l$).
- Page 109. In the next-to-last paragraph, the formula of the inverse NTT misses a factor $L^{-1} \bmod p = -\nu$ and the subscript of T should be j. The correct formula is $t_i = -\nu \sum_{j=0}^{L-1} T_j \omega^{-ij}$.
- Page 109. In the last paragraph, one should read: *In $\mathbf{Z}_{786\,433}$, **a possible generator** is $g = 11$* [...]. The smallest generator is in fact $g = 10$, although any generator can be used.

In the bibliography

- Page 250. In entry [22], the correct page numbers are **487–496**.
- Page 256. In entry [149], the authors are: G. Ribordy, J.-D. Gautier, N. Gisin, **O. Guinnard** and H. Zbinden.