Foundations of Cryptography
errors and comments on the Fragments

Oded Goldreich
oded@wisdom.weizmann.AC.IL
Computer Science and Applied Math. Dept.
Weizmann Institute of Science
Rehovot, Israel.

April 23, 1996

1. The statement of Hoefding Inequality (page 22) is wrong. The correct statment is

$$\mathrm{Prob}\left(\left|\frac{\sum_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{X_i}}{\mathrm{n}} - \mu\right| > \delta\right) < 2 \cdot \mathrm{e}^{-\frac{2\delta^2}{(\mathrm{b}-\mathrm{a})^2}\cdot \mathrm{n}}$$

   Pointed out by Erez Petrank.

2. Definition of polynomial-time enumerable sets (page 39) should require the output, $s_I(n)$ to be in unary so that $s_I(n) = \mathrm{poly}(n)$ holds (as stated on page 41). Pointed out by Daniele Micciancio.

3. Exercises 10 and 11 in Chapter 2 are phrased in a careless manner. Firstly, one should quantify only on probabilistic polynomial-time algorithms. Secondly, in Exercise 10 some negations are missing: each algorithm fails with non-negligible probability (rather than negligible one) and the hint should be corrected accordingly.

4. Exercise 23 in Chapter 3 ("alternative definition of of pseudorandom functions") is wrong. Consider, for example, a pseudorandom function modified so that $f(0^n) = 0$. The resulting function ensemble will pass the test, but is not pseudorandom. A generalization, in which $f(f(0^n))$ is set to zero (instead of setting $f(0^n)$ to zero) can be used to kill attempts for amending the "alternative definition". Pointed out by Omer Reingold.

5. There was an error in the definition of a perfect bit commitment scheme (Definition 6.57 on page 220). When defining a feasible σ-opening (with respect to algorithm F^*) one only gives $(\overline{m}, s, \tilde{m}, \sigma)$ as input to F^* (rather than providing F^* also with r).