Correction (PSEC speficication)

In the current version, the following typos in the original version were corrected:

In subsections 4.1, 6.1, 7.1 and 8.1, $q = p^n$ (p: prime) was corrected by $q = {q_0}^n$ (q_0: prime), and $\mathbf{Z}/p\mathbf{Z}$ was corrected by $\mathbf{Z}/q_0\mathbf{Z}$ in the same paragraph.