Errata/Typos for “Introduction to Modern Cryptography, third edition”

(Last updated July 23, 2024)

Note: negative line numbers correspond to counting from the bottom of the page.

- page 58, Theorem 3.11: f should be computable in polynomial time.
- page 170: as indicated in Exercise 6.1(b), second-preimage resistance implies preimage resistance only under certain additional conditions; it is not true in general.
- page 252, line -2 of Construction 7.6: z_i^* should be y_i^*.
- page 283, line 11: $\hat{G}(s)$ should be $G(s)$.
- page 362, Exercise 9.24: For this problem, assume that the twisted Edwards representation uses quadratic residue a and quadratic non-residue d.
- page 368, line 8: “less than p_k” should be “at most p_k.”
- page 449, line -10: k_1 should be k.
- page 450, line -4 of Construction 12.36: should read $s \in \{0,1\}^k$ and $t \in \{0,1\}^{\ell+k}$.
- page 483, line -7: $g^{\alpha(s_1^{-1}-s_2^{-1})} = y^{r_1 s_1^{-1} - r_2 s_2^{-1}}$ should be $g^{\alpha(s_1^{-1}-s_2^{-1})} = y^{r_2 s_2^{-1} - r_1 s_1^{-1}}$.
- page 501, line -12: should read “. . . we can let C be the set of all strings whose first $m - \log \ell$ bits are all 0 and take D to be the set of all strings whose first $m - 2\log \ell$ bits are all 1.”
- page 507, last displayed equation: e_{n+1} should be $\hat{e}_{n+1}$.
- page 577, line -7 should have “$\geq$” instead of “$\leq$.” In any case, the only result we rely on is that when the $\{E_i\}_{i=1}^n$ are disjoint events with $\Pr[\vee_{i=1}^n E_i] = 1$, then for any event F we have

$$\Pr[F] = \sum_{i=1}^{n} \Pr[F \bigwedge E_i] = \sum_{i=1}^{n} \Pr[F \mid E_i] \cdot \Pr[E_i].$$

- page 578, line 17: X_i should be X_1 and X_j should be X_2.

Thanks to Paulo Barreto, Claude Crépeau, Owen Ekblad, Bruno Grenet, Dominique Schröder, Marek Sefranek, Patrick Struck, and Bingsheng Zhang for informing us about some of the above typos.