Errata/Typos for "Digital Signatures"

(Last updated January 28, 2019)

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

- Page 25, lines 2 and 4: PK should be pk.
- Page 25: footnote 3 appears to be incorrect.
- Page 27, line 7: pk'_{i^I} should be pk'_{i^*}.
- Page 38, line 3: $I \in D_I$ should be $x \in D_I$.
- Page 104, line 2: s_v should be $s_{v_{r-1}}$.
- Page 105, line 2: $y^{\hat{e}}$ should be $y^{L_w \cdot \hat{e}}$. And on line 3, $y^{\hat{e}/e_i}$ should be $y^{L_w \cdot \hat{e}/e_i}$.
- Page 115, line 1 after Construction 4.7: "compute $e_j \ldots$ for $j \in \{1, \ldots, t\} \setminus \{i\}$" should be "compute $e_i \ldots$ for $i \in \{1, \ldots, t\} \setminus \{j\}$."
- Page 115, lines 12–14 after Construction 4.7: α should be α_i.
- Page 118, line 14: "and strong unforgeability" should be "implies strong unforgeability".
- Page 129, line 9: The beginning of that line should read "$\ldots$ setting $|S|/2^k \approx \left(1 - \frac{1}{q_s}\right)$ then gives B success probability $O(\varepsilon/q_s)$."

  It should also be clear that the discussion there is meant *just* as intuition, and does not reflect the actual analysis nor the concrete reduction obtained.
- Page 130, line 9: In the denominator, $g^G(m)$ should be $g^{G(m)}$.
- Page 145, line -11: $\mathsf{Samp}(I, r)$ should be $\mathsf{Samp}(I; r)$.
- Page 148, line -11: $b_i := 2$ should be $b_i := 1$.
- Page 181, line 11: (A, c, r) should be (I, c, r).

Thanks to Masayuki Abe, Yi Liu, and Wei Ren for sending some of the above corrections.