

Table with 3 columns: Location, Original, and Change. It lists various errors from the book, such as typos, missing definitions, and incorrect mathematical statements, along with their corrections.

Table with 3 columns: Location, Original, and Change. It continues the list of errors and corrections, including issues with algorithm descriptions and mathematical derivations.

Table with 3 columns: Location, Original, and Change. It covers errors related to the RSA signature scheme, including issues with the signing process and verification steps.

Table with 3 columns: Location, Original, and Change. It addresses errors in the final sections of the book, including the discussion on the security of the RSA signature scheme.

In case the attacker does not know the exact fault mask  $\epsilon$  (and hence does not know  $n'$ ), but instead knows only a range of possible values for  $\epsilon$ , then we have to try all possible values of  $\epsilon$  together with all possible bit guesses in Equation 3.1 in order to reduce the set of key candidates. We refer the readers to [BCC08] for more details.