B. Changelog

- 29-03-2019: version v1.0
- 06-06-2019: version v1.01
  - added link to webpage and GitHub
- 22-07-2019: version v1.1
  - added an improved authenticity bound of Romulus-N in Section 4.2, and a corrected and improved nonce-misusing authenticity bound of Romulus-M in Section 4.3. Both improvements are based on the analysis in [35], and the analysis on Romulus-M is also based on [15].
  - added Section 2.5.5 to describe some possible options for a cryptographic hash function based on Skinny.
- 20-09-2019: version v1.2
  - added two paragraphs in Section 6 on how the design choices relate to the serial low-area hardware implementations. Added Figure 6.2.
  - added the synthesis results for the low area implementation in Table 7.1.