Angewandte Kryptographie 2 Prof. Dr.-Ing. Kerstin Lemke-Rust
SoSe 2023 Hochschule Bonn-Rhein-Sieg

Computerpraktikum: Aufgabenblatt 3

C.1 Experimentieren Sie mit der Referenzimplementierung von XMSS von `https://github.com/XMSS/xmss-reference`.

(a) Kompilieren Sie die Referenzimplementierung (make), installieren Sie ggf. Abhängigkeiten von OpenSSL.

(b) Analysieren Sie Performance und den Ressourcenbedarf für die Parametersätze

- XMSS-SHA2_10_256,
- XMSS-SHA2_16_256,
- XMSS-SHAKE256_10_256,
- XMSS-SHAKE256_16_256,
- XMSSMT-SHA2_20/2_256 und
- XMSSMT-SHAKE256_20/2_256

der NIST SP800-208. Verwenden Sie hierfür z.B. die Datei test/speed.c als Basis.