Documentation of a protected implementation

1. Protection Method

   (a) All designs are based on PINI-secure, composable “Hardware Private Circuits 2” (HPC2) gadgets. We create such designs by using a tool for “Automated Generation of Masked Hardware” (AGEMA).

   (b) Hardware Private Circuits: https://eprint.iacr.org/2020/185.pdf
   Automated Generation of Masked Hardware: https://eprint.iacr.org/2021/569.pdf