IntegriKey (2017, eprint: 2017/1245)

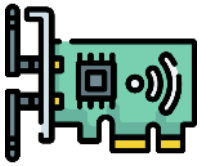
IntegriScreen (2018, arXiv:2011.13979)

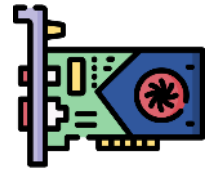
ProtectION (NDSS 2020)

PIE (2020, arXiv:2010.10416)

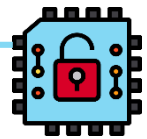
Remote system

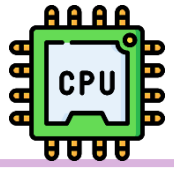
Remote trusted path application





Dedicated Security Chips in the Age of Secure Enclaves (IEEE S&P magazine 2020)





Platform identitity

ProximiTEE (CODASPY 2020)