

Known
Ajper
Tests
.rsp
rng.h
??
pk
sk
ss
kat, basicstyle =
|kyber512count =
0seed =
632616E53E5C162547070F037A3C4D2644D25C6552272846174A698762514332pk =
753F88E022567D07...[truncado]...A3273187FDD077sk =
826F8082692F0197...[truncado]...A3273187FDD077ct =
7219927A685D26C3...[truncado]...E5D79E182D2D70ss =
A3D3F1E38367A58E29E250A84D5852267667C08CC3B44B36398F81716A8C576D

platform Evaluacin comparativa del coste computacional (ciclos de reloj) de los esquemas HQC, Kyber y Saber, segregado por device Impacto de la forma de ejecucin en el nmero de ciclos de CPU requeridos por cada algoritmo postcuntico individual.

platform Evaluaciⁿ comparativa del caudal de procesamiento (operaciones por segundo) de los esquemas HQC, Kyber y Saber device Impacto de la arquitectura de hardware en el rendimiento computacional (operaciones por segundo) para cada algoritmo

platform Evaluacióncincomparativadelconsumodepila(stackusage)delosesquemashqc, Kyber y Saber, segregadoporplataforma device Impactodelaarquitecturadehardwareenlosrequerimientosdememoriadepilaparacadaalgoritmopostcunticoindividuo