

ZKP-SOC技术参数来自华为检测

MOD	芯片 计算时间 (ms) (芯片内部时钟)	
尺寸	MOD_ADD	Mod_sub
2*14	0.29	0.29
2*15	0.29	0.29
2*16	0.35	0.36
2*17	0.63	0.62
2*18	1.21	1.23
2*19	2.37	2.37
2*20	4.84	5.02
2*21	10.29	10.51
2*22	21.38	21.46
2*23	39.13	39.63
2*24	75.94	75.82
2*25	143.91	144.26
2*26	286.77	286.67

ZKP-SOC-MOD性能参数



MOD（模运算）
在ZKP-SOC芯片
功能优势

MOD功能优势

增强安全性 提高计算效率 优化资源利用

MOD	芯片 计算时间 (ms) (芯片内部时钟)	
尺寸	ModMul-ADD	ModMul-ASub
2*14	0.29	0.29
2*15	0.29	0.29
2*16	0.44	0.44
2*17	0.81	0.81
2*18	1.55	1.58
2*19	3.04	3.02
2*20	6.26	6.25
2*21	12.88	12.63
2*22	25.42	25.70
2*23	49.42	48.51
2*24	94.428	93.93
2*25	183.57	184.31
2*26	427.47	424.58