ELECTRA IC
Design & Verification

Crypto IP Cores

IP	Modes of Operation / Notes	LUT/DSP/BRAM	Max Clock Frequency on Z-7045 (speed grade -1)	Transaction per Second (TPS) / Throughput without SCA countermeasure *	Transaction per Second (TPS) / Throughput with SCA countermeasure *	Certification / Compliant Standards	Side-channel Counter measure	Tested on
AES	ECB, CBC, CTR, GCM	4087/0/3	206 MHz	~20M (ECB-128)	~7.5M (ECB-128)	Certified by PCI for having counter measure to side-channel attacks. (NIST FIPS) - 197	Yes	Z-7015 Z-7020 Z-7045
TDES	ECB, CBC	2163/0/3	178 MHz	~11M (ECB-64)	~11M (ECB-64)	Certified by PCI for having counter measure to side-channel attacks.	Yes	Z-7015 Z-7020 Z-7045
TRNG	NA	431/0/1	300 MHz	300Mbit/s	NA	NIST 800-90B, NIST 800-22, AIS-20/31	No	Z-7015 Z-7020 Z-7045
DRBG	NA	2247/0/1	188 MHz	2Gbit/s	NA	NIST 800-90A	No	Z-7015 Z-7020 Z-7045
HASH	MD5, SHA, SHA224, SHA256, SHA384, SHA512	4736/0/1	111 MHz	875.21 Mbit/s	NA	FIPS 180-4	No	Z-7015 Z-7020 Z-7045
SHA3	SHA3_224, SHA3_256, SHA3_384, SHA3_512, SHAKE128, SHAKE256	5130/0/1	300 MHz	106268 (SHA3-256 Min. Msg Hash per second)	NA	FIPS 202	No	Z-7015 Z-7020 Z-7045
RSA Sign/Verify	Composed of multiple Montgomery Modulo Exponential Cores, RISC-V, and a DMA core	155733/900/258	215 MHz	12015 TPS (RSA Sign 2048-bit)	NA	FIPS 186-3	No	Z-7015 Z-7020 Z-7045
RSA Keygen	512 - 2048 bit	26100/0/26	215 MHz	2.5 - 3 (2048 bit)	NA	FIPS 186-3	No	Z-7015 Z-7020 Z-7045
ECDSA Sign	NIST (192, 224, 256, 384, 521)P	132715/883/191	220 MHz	15000(ECDSA Sign NIST256p)	NA	FIPS 186-3	No	Z-7015 Z-7020 Z-7045

** Throughput and TPS information is given for **Z-7045 FPGA-SoC**.*