Product Type	Integrated Communication Processor
NXP Part #	LS2088A, LS2084A
Package	37.5mm x 37.5 mm, 1292 flip-chip plastic ball grid array (FC-PBGA)
Crypto Hardware	SEC 5.1

Algorithms	**Max Key Size (bits)**
DES (ECB, CBC, OFB, CFB)	56
3DES (ECB, CBC, OFB, CFB)	168 (3-keys)
AES (ECB, CBC, CTR, CCM, CMAC, GCM, OFB, CFB, XCBC-MAC)	256
MD-5 + HMAC	(up to 512 bit keys)
SHA-1 + HMAC	(up to 512 bit keys)
SHA-224 + HMAC	(up to 512 bit keys)
SHA-256 + HMAC	(up to 512 bit keys)
SHA-384 + HMAC	(up to 512 bit keys)
SHA-512 + HMAC	(up to 512 bit keys)
Kasumi (A5/3, GEA-3, f8, f9)	128
Snow 3G	128
ZUC (EEA-1 & EIA-2)	128
RSA Digital Signature	4096-bit operands
RSA Digital Verify	4096-bit operands
ECC Digital Signature	1023-bit field or modulus size
ECC Digital Verify	1023-bit field or modulus size
FIPS compliant deterministic RNG	On chip 32-bit

Target Applications :
Combined control, data path,and application layer processing in routers, switches, gateways, and general-purpose embedded computing systems.

Export Control Info:
Harmonized Tariff (US): 8542.31.0000
ENC Status: Restricted. US EAR part 740.17(b)(2)
ECCN: 5A002A.1
CCAT: G153895

Overview:
The LS2088A and LS2084A are members of the QorIQ Layerscape family of integrated communications processor from NXP Semiconductor.

The LS2088A incorporates (8) 64b A72 ARM Architecture CPU cores, (2) 64b and (1) 32b DDR4 Memory Controllers, (8) 10G Ethernet and (8) 1G Ethernet controllers, along with multiple PCIe and other peripheral bus controllers. The LS2088A incorporates the AIOP (Advanced IO Processor), a C-programmable packet processing engine.

The LS2084A incorporates (8) 64b A72 ARM Architecture CPU cores, (2) 64b DDR4 Memory Controllers, (8) 10G Ethernet and (8) 1G Ethernet controllers, along with multiple PCIe and other peripheral bus controllers.

In addition to these CPUs and interfaces, the LS2088A and LS2084A integrate a 10Gbps Decompress/Compress Engine (DCE 1.0), a 10Gbps Pattern Matching (RegEx) Engine (PME 2.0), and a 20Gbps Crypto Acceleration Engine (SEC 5.1). The algorithms and key lengths supported by the SEC 5.1 are listed in the table above.

In addition to crypto algorithm processing, the SEC 5.1 supports security protocol processing off-load capability, with specific support for protocol header and trailer processing for IPsec, SSL, DTLS, SRTP, MACSec, 802.16e, and 802.11e. The SEC 5.1 is expected to achieve 5000+ public key exchanges per second.

The LS2088A & LS2084A also provide support for secure boot and platform assurance, including ARM TrustZone.

NOTE 1: This authorization does not authorize the export of products designed to use the encryption functionality of these chips. Such products may require a classification and/or license from the Bureau of Industry and Security (BIS) prior to export. OEMs incorporating these chips in their products should call the BIS Encryption Export Support Line at 202-482-0707 with specific questions.

NOTE 2: NXP Semiconductor ("NXP") makes this export classification and regulatory information available for informational purposes only. It may not reflect the most current legal developments, and NXP does not represent, warrant or guarantee that it is complete, accurate or up-to-date. This information is subject to change without notice. The contents of this fact sheet are not intended to constitute legal advice or to be used as a substitute for specific legal advice from a licensed attorney and or customs broker. You should not act or refrain from acting based upon information in this email without obtaining professional advice regarding your particular facts and circumstances.