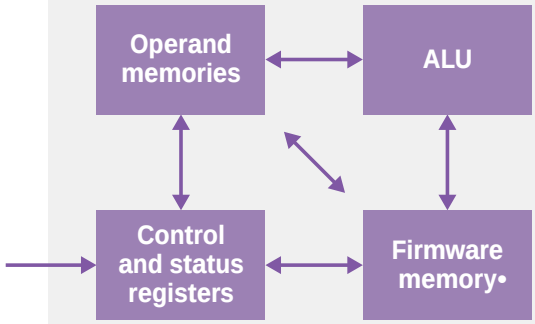
Overview

Public key cryptography requires complex mathematical operations on very large numbers (from 160 to 4096 bits, or more). The majority of embedded CPUs are limited to operations on 32- and 64-bit values and require significant computational resources when implementing public key infrastructure related algorithms. The DesignWare® Public Key Accelerator (PKA) is dedicated to the computationally intensive elements of the mathematics required for RSA operations as well as the algorithms used in prime field elliptic curve cryptography (ECC). The PKA integrates seamlessly with the DesignWare cryptography software library, enabling designers to accelerate the asymmetric cryptography required in public key algorithms, to deliver performance levels that are not achievable in software-only solutions.

DesignWare Public Key Accelerator

The traditional RSA, digital signature algorithm (DSA), and Diffie-Hellman (DH) asymmetric algorithms require the calculation of complex modular exponentiation operations to encrypt, decrypt, sign, and verify data for public key negotiations or digital signature schemes. Similarly, ECC requires a number of complex mathematical operations, such as point multiplications, in support of public key negotiations and digital signature schemes.



32A	27	1280	187	N/A	323	N/A
32B	27	2560	187	32	323	60
64A	55	1280	381	N/A	408	N/A
64B	55	2560	381	92	408	116
128A	120	1280	605	N/A	470	N/A
128B	120	2560	605	195	470	169

- 40-nm at 340 MHz
- Firmware memory size not included
- RSA performance does not include pre-processing
- Full operand size, 50% hamming weight

Table 1: Typical Public Key Accelerator buil.4 (i)14 (n)17.2 (c)19.1 (l)14.5 (u)182cT-0.169