BERTEN Digital Signal Processing

PKEC-P521 IP Core

Public Key Crypto Core

Elliptic Curve Cryptography (ECC)

Up to 1008-bit Curves

Low Resource Utilisation

Register-based Configuration

Features

- ECDH, ECDSA, EC-KCDSA
- Prime Fields up to 1008 Bits
- NIST, SECG, Brainpool Curves
- Curve25519, Curve448
- NIST SP800-56A Compliant
- FIPS 186-5 & ISO 14888-3 Compliant
- SPA and DPA Countermeasures
- Fault Injection Resistance
- Portable to any FPGA or ASIC
- AMBA AXI Interface

Applications

- Network Security: MACsec, IPsec
- Transport Protocols: TLS, SSL
- CPU Crypto Acceleration
- User Authentication
- Secure Communications
- Electronic Transactions

The **PKEC-P521** is a Public Key Accelerator IP Core for hardware offloading of Elliptic Curve Cryptography (ECC) in FPGA, SoC, and ASIC technologies.

The core implements ECDH (Elliptic Curve Diffie–Hellman) Key Exchange, ECDSA (Elliptic Curve Digital Signature Algorithm), and EC-KCDSA (Korean Certificate-based Digital Signature Algorithm).

It supports ECC operations up to 1008 bits in prime fields, F(p). Any elliptic curve in Short-Weierstrass form can be configured, including NIST, Brainpool, SECG, Curve25519, Curve448, Montgomery, and Twisted-Edwards curves.

Portable to any Xilinx, Intel, or Microsemi device, the PKEC-P521 is compliant with NIST SP800-56A (Rev.3), FIPS 186-5, and ISO 14888-3:2018.

The public key crypto core implements strong protections against Fault Injection and Side-Channel Attacks (SCA), including SPA and DPA countermeasures.

PKEC-P521 includes an AXI4-Lite interface and a register map with user-programmable parameters to select the ECC operation, configure the Elliptic Curves, and exchange I/O data. ANSI C drivers are provided for a fast integration into the target platform.

www.bertendsp.com sales@bertendsp.com +34 942 18 10 11

Elliptic Curve Operations

PKEC-P521 includes ECDH, ECDSA, and EC-KCDSA algorithms to support key exchange and signature operations based on any Short-Weierstrass elliptic curve up to 1008 bits in prime fields, including:

- NIST: P-192, P-224, P-256, P-384, P-521
- Brainpool: P192r1, P224r1, P256r1, P320r1, P384r1, P512r1
- SECG: secp192k1, secp192r1, secp224k1, secp224r1, secp256k1, secp256r1, secp384r1, secp521r1
- Curve25519, Curve448

The core implements a sequencer and a SCA-protected arithmetic unit in a minimum area. Random nonces, private and public keys, hash values, and signatures are exchanged through the integrated register map.

	ECC Operation	Performance, op/s 256-bit Curve @300MHz
ECDH	Public Key Generation from Private Key	111
	Shared Key Generation	101
ECDSA	Public Key Generation from Private Key	111
	Signature Generation	100
	Signature Verification	55
EC-KCDSA	Public Key Generation from Private Key	101
	Signature Generation	111
	Signature Verification	58

Attack Resistance

The IP core implements countermeasures against Fault Injection and Side-Channel Attacks (SCA), including Timing, Simple (SPA), and Differential Power Analysis (DPA) attacks.

PKEC-P521 reports an alarm when the input values are invalid or unsafe. Automatic and on-demand zeroization of internal memories and registers are also available.

Resources

Resource utilisation for different devices is provided in the table below. Metrics for any Xilinx, Intel, or Microsemi FPGA or SoC are available as required.

	Device Family	LUT	Register
Xilinx	Spartan-7, Artix-7, Kintex-7, Virtex-7	3.0K	2.6K
	Kintex/Virtex Ultrascale	2.8K	2.6K
	Kintex/Virtex Ultrascale+	2.9K	2.6K
	Versal ACAP	2.8K	2.7K
Intel	MAX 10 / Cyclone 10 LP	5.8K	2.6K
	Cyclone V	3.1K	2.8K
	Arria 10	3.1K	2.7K
	Stratix V	3.2K	2.8K

Interfaces

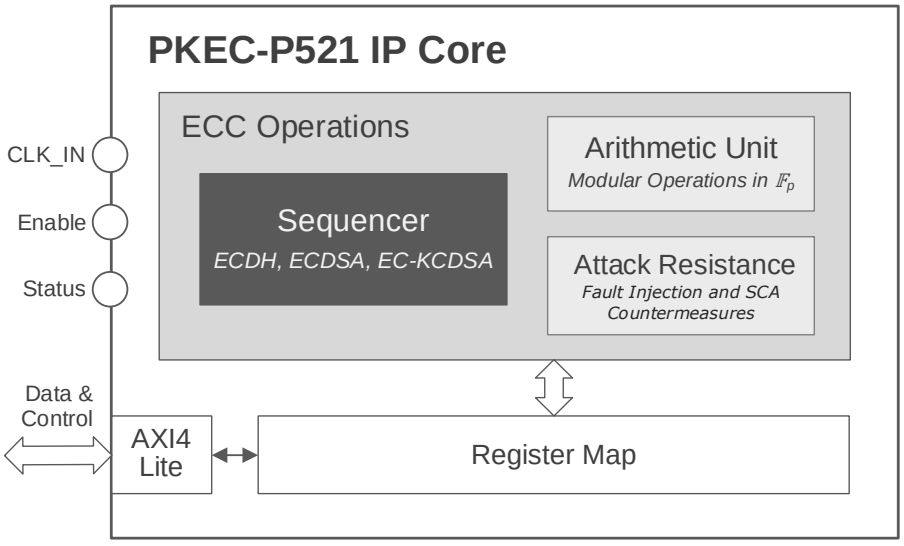
The AXI4-Lite interface provides access to the register map to select the ECC operation mode, configure the domain parameters (Field and Elliptic Curve), and exchange I/O data. A Status port is available for events notification.

Licensing

The IP Core is provided as encrypted netlist for one device family, under a perpetual Site Licence. It includes 12 months of maintenance and support for the integration of the module in your platform.

Deliverables

- Targeted, timing closed Netlist
- Design Constraints
- User Manual
- ANSI C drivers



www.bertendsp.com sales@bertendsp.com +34 942 18 10 11