Bit number				31 30 29 28 27 26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
ID				L K J I H G F E E E D C C C C C C C C C B A A A A A A A
Reset 0x0000000F				**0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1**
ID	R/W	Field	Value ID	Value	Description
C	RW	OPBYTESM1			This field defines the size (= number of bytes minus one) of the operands for the current operation. Possible values are limited by the maximum supported operand size. Examples: - 0x014 - ECC on curve K-163 - 0x01F - ECC on curve P-256 - 0x02F - ECC on curve P-384 - 0x033 - ECC on curve K-409 - 0x041 - ECC on curve P-521 - 0x07F - 1024-bit RSA - 0x09F - 1280-bit RSA - 0x1FF - 4096-bit RSA - 0x3FF - 8192-bit RSA
D	RW	RANDMOD			Enable randomization of modulus (counter-measure).
E	RW	SELCURVE			Enable accelerator for specific curve modulus: This field has no effect when the optional acceleration hardware is not included.
			NOACCEL	0x0	No acceleration (default)
			P256	0x1	P256
			P384	0x2	P384
			P521	0x3	P521
			P192	0x4	P192
			CURVE25519	0x5	Curve25519
			ED25519	0x6	Ed25519.
F	RW	RANDKE			Enable randomization of exponent/scalar (counter-measure).
G	RW	RANDPROJ			Enable randomization of projective coordinates (counter-measure).
H	RW	EDWARDS			Enable Edwards curve.
I	RW	SWAPBYTES			Swap the bytes on AHB interface: This bit must be programmed before writing/reading any data in data memory.
			NATIVE	0	Native format (little endian).
			SWAPPED	1	Byte swapped (big endian).
J	RW	FLAGA			Flag A.
K	RW	FLAGB			Flag B.
L	RW	CALCR2			This bit indicates if the IP has to calculate R**2 mod N for the next operation. This bit must be set to 1 when a new prime number has been programmed. This bit is used for primitive operations and ignored for the other operations.
			NRECALCULATE	0	don't recalculate R^2 mod N
			RECALCULATE	1	re-calculate R^2 mod N

7.8.1.7.45 PK.CONTROL

Address offset: 0x2008

Command register.

Bit number				31 30 29 28 27 26 25 24 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
ID				B A
Reset 0x00000000				**0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0**
ID	R/W	Field	Value ID	Value	Description
A	W	START			Writing a 1 starts the processing.
B	W	CLEARIRQ			Writing a 1 clears the IRQ output.