

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				C B A A A A A A A A																															
Reset 0x00000337				0 1 1 0 0 1 1 0 1 1 1																															
ID	R/W	Field	Value ID	Value				Description																											
A	R	NUMBOFRINGS						Generic g_NumRings value.																											
B	R	AIS31						Generic g_AIS31 value.																											
C	R	AIS31FULL						Generic g_AIS31Full value.																											

7.8.1.7.42 RNGCONTROL.FIFO[n] (n=0..15)

Address offset: 0x1080 + (n × 0x4)

FIFO data

The FIFO contains the RNG output data.

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				A A																															
Reset 0x00000000				0 0																															
ID	R/W	Field	Value ID	Value								Description																							
A	R	DATA										FIFO data																							

7.8.1.7.43 PK.POINTERS

Address offset: 0x2000

Pointers 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				D D D D								C C C C				B B B B				A A A A															
Reset 0x00000000				0 0																															
ID	R/W	Field	Value ID	Value				Description																											
A	RW	OPPTRA						When executing primitive arithmetic operations, this pointer defines where operand A is located in memory (location 0x0 to 0xF).																											
B	RW	OPPTRB						When executing primitive arithmetic operations, this pointer defines where operand B is located in memory (location 0x0 to 0xF).																											
C	RW	OPPTRC						When executing primitive arithmetic operations, this pointer defines the location (0x0 to 0xF) where the result will be stored in memory.																											
D	RW	OPPTRN						When executing primitive arithmetic operations, this pointer defines the location where the modulus is located in memory (location 0x0 to 0xF).																											

7.8.1.7.44 PK.COMMAND

Address offset: 0x2004

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				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																											
A	RW	OPEADDR						This field defines the operation to be performed.																											
								See documentation for more details.																											
B	RW	FIELDF						0: Field is GF(p) 1: Field is GF(2**m)																											