Status and Control

Status Register (SR) 0x0000

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
Res	Res	Res	Res	Res	Res	Res	Res	Res	Res	Res	Res	Res	Res	Res	Res

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Res	Res	Res	Res	Res	Res	Res	Res	Res	Res	Res	Res	BSY	STATE [2:0]		
								r	r	r	r	r	r	r	r

Bits [31:4]: Reserved

Bit 3: **BSY** Busy status bit. This bit is high when the ASCON core is doing a computation

Bits [2:0]: **STATE** Current state of ASCON core

000: idle

001: initialize

010: AD (Associated Data)

011: PT (Plaintext Encrypt)

100: CT (Ciphertext Decrypt)

101: finalize

110: unused

111: unused

Control Register (CR) 0x0004

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
Res	Res	Res	Res	Res	Res	Res	Res	Res	Res	Res	Res	Res	Res	Res	Res

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
STRT	MODE [1:0]		ADLEN [4:0]					DATALEN [7:0]							
rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw

Bits [31:16]: Reserved

Bit 15: **STRT** start ASCON operation

Bits [14:13]: **MODE** operational mode of ASCON core

00: No associated data, decrypt

01: No associated data, encrypt

10: Yes associated data, decrypt

11: Yes associated data, encrypt

Bits [12:8]: **ADLEN** Length in bytes of Associated Data

Bits [7:0]: **DATALEN** Length in bytes of data input

Input Data

Key Registers 0-3 0x0008-0x0014

Key Reg0 (KR0) 0x0008

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
KEY1 [15:0]															
rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
KEY0 [15:0]															
rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw

Bits [31:16]: **KEY1** Bits [31:16] of the secret key
Bits [15:0]: **KEY0** Bits [15:0] of the secret key

Key Reg1 (KR1) 0x000C

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
KEY3 [15:0]															
rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
KEY2 [15:0]															
rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw

Bits [31:16]: **KEY3** Bits [63:48] of the secret key
Bits [15:0]: **KEY2** Bits [47:32] of the secret key

Key Reg2 (KR2) 0x0010

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
KEY5 [15:0]															
rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
KEY4 [15:0]															
rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw

Bits [31:16]: **KEY5** Bits [95:80] of the secret key
Bits [15:0]: **KEY4** Bits [79:64] of the secret key

Key Reg3 (KR3) 0x0014

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
KEY7 [15:0]															
rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
KEY6 [15:0]															
rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw

Bits [31:16]: **KEY7** Bits [127:112] of the secret key
Bits [15:0]: **KEY6** Bits [111:96] of the secret key

Nonce Registers 0-3 0x0018-0x0024

Nonce Reg0 (NR0) 0x0018

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
NONCE1 [15:0]															
rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
NONCE0 [15:0]															
rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw

Bits [31:16]: **NONCE1** Bits [31:16] of the nonce
Bits [15:0]: **NONCE0** Bits [15:0] of the nonce

Nonce Reg1 (NR1) 0x001C

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
NONCE3 [15:0]															
rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
NONCE2 [15:0]															
rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw

Bits [31:16]: **NONCE3** Bits [63:48] of the nonce
Bits [15:0]: **NONCE2** Bits [47:32] of the nonce

Nonce Reg2 (NR2) 0x0020

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
NONCE5 [15:0]															
rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
NONCE4 [15:0]															
rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw

Bits [31:16]: **NONCE5** Bits [95:80] of the nonce
Bits [15:0]: **NONCE4** Bits [79:64] of the nonce

Nonce Reg3 (NR3) 0x0024

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
NONCE7 [15:0]															
rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
NOCNE6 [15:0]															
rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw

Bits [31:16]: **NONCE7** Bits [127:112] of the nonce
Bits [15:0]: **NONCE6** Bits [111:96] of the nonce

Associated Data Registers 0-3 0x0028-0x0034

Associated Data Reg0 (ADR0) 0x0028

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
AD0_1 [15:0]															
rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
AD0_0 [15:0]															
rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw

Bits [31:16]: **AD0_1** Bits [31:16] of the first associated data block
Bits [15:0]: **AD0_0** Bits [15:0] of the first associated data block

Associated Data Reg1 (ADR1) 0x002C

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
AD0_3 [15:0]															
rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
AD0_2 [15:0]															
rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw

Bits [31:16]: **AD0_3** Bits [63:48] of the first associated data block
Bits [15:0]: **AD0_2** Bits [47:32] of the first associated data block

Associated Data Reg2 (ADR2) 0x0030

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
AD1_1 [15:0]															
rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
AD1_0 [15:0]															
rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw

Bits [31:16]: **AD1_1** Bits [31:16] of the second associated data block
Bits [15:0]: **AD1_0** Bits [15:0] of the second associated data block

Associated Data Reg3 (ADR3) 0x0034

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
AD1_3 [15:0]															
rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
AD1_2 [15:0]															
rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw	rw

Bits [31:16]: **AD1_3** Bits [63:48] of the second associated data block
Bits [15:0]: **AD1_2** Bits [47:32] of the second associated data block

Output Data

Tag Registers 0-3 0x0038-0x0044

Tag Reg0 (TR0) 0x0038

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
T1 [15:0]															
r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
T0 [15:0]															
r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r

Bits [31:16]: **T1** Bits [31:16] of the tag
Bits [15:0]: **T0** Bits [15:0] of the tag

Tag Reg1 (TR1) 0x003C

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
T3 [15:0]															
r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
T2 [15:0]															
r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r

Bits [31:16]: **T3** Bits [63:48] of the tag
Bits [15:0]: **T2** Bits [47:32] of the tag

Tag Reg2 (TR2) 0x0040

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
T5 [15:0]															
r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
T4 [15:0]															
r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r

Bits [31:16]: **T5** Bits [95:80] of the tag
Bits [15:0]: **T4** Bits [79:64] of the tag

Tag Reg3 (TR3) 0x0044

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
T7 [15:0]															
r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r
15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
T6 [15:0]															
r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r

Bits [31:16]: **T7** Bits [127:112] of the tag
Bits [15:0]: **T6** Bits [111:96] of the tag

Memory Scratchpad

Reading / writing to addresses 0x0048-0x00C4 will access to RAM block. These adresses are used to store the plaintext and ciphertext data. The user will load the plaintext / ciphertext (depending on the mode) and it will be overwritten by the complementary data such that it can be read back. For example, if the user writes 2 blocks of plaintext data to the RAM and then runs ASCON encryption, the first four addresses of RAM will be overwritten with the ciphertext.