Each Cryptech core has a set of 4-byte registers, which are accessed through a 16-bit address. The address space is divided as follows:

• 3 bits segment selector	up to 8 segments
• 5 bits core selector	up to 32 cores/segment (see note below)
• 8 bits register selector	up to 256 registers/core

i.e, the address is structured as:

```
sss ccccc rrrrrrrr
```

The I2C and UART communication channels use this 16-bit address format directly in their read and write commands.

The EIM communications channel translates this 16-bit address into a 32-bit memory-mapped address in the range 0x08000000..807FFFF:

```
0000 1000 0000 0sss 0ccc ccrr rrrr rr00
```

EIM, as implemented on the Novena, uses a 19-bit address space:

- Bits 18..16 are the segment selector.
- Bits 15..10 are the core selector.
- Bits 9..2 are the register selector.
- Bits 1..0 are zero, because reads and writes are always word aligned.

Note that EIM can support 64 cores per segment, but we sacrifice one bit in order to map it into a 16-bit address space.

The current memory map is described in the following table. This is derived from cryptech.h, which is in turn derived from addresses and values defined in the various Verilog core_selector and core wrapper files. In the case of inconsistencies between the documents, the Verilog wins, because that's what's actually running on the FPGA.

EIM addresses are provided for informational use only. The API uses the 16-bit register addresses exclusively, and only converts to EIM addresses internally.

Also, please use the symbolic names instead of the numeric addresses and values (e.g. AES_ADDR_CONFIG instead of 0x6008).

seg	core	reg	reg addr	EIM addr	name	description
00 Global	00 Board	00	0000	08000000	board_name0	"PVT1"
		01	0001	08000004	board_name1	" "
		02	0002	08000008	board_version	"0.10"
		ff	00ff	080003fc	board_dummy	Dummy read/write register
	01 Communications channel	00	0100	08000400	comm_name0	"eim " or "i2c "
		01	0101	08000404	comm_name1	" "
		02	0102	08000408	comm_version	"0.10"
01 Hash	00 SHA-1	00	2000	08010000	sha1_name0	"sha1"
		01	2001	08010004	sha1_name1	" "
		02	2002	08010008	sha1_version	"0.50"
		08	2008	08010020	sha1_ctrl	bit 0 = init, bit 1 = next
		09	2009	08010024	sha1_status	bit 0 = ready, bit 1 = valid
		10	2010	08010040	sha1_block0	Input data block
		…	…	…	…	
		1f	201f	0801007c	sha1_block15	
		20	2020	08010080	sha1_digest0	Output message digest
		…	…	…	…	
		24	2024	08010090	sha1_digest4	
	01 SHA-256	00	2100	08010400	sha256_name0	"sha2"
		01	2101	08010404	sha256_name1	"-256"
		02	2102	08010408	sha256_version	"0.80"
		08	2108	08010420	sha256_ctrl	bit 0 = init, bit 1 = next
		09	2109	08010424	sha256_status	bit 0 = ready, bit 1 = valid
		10	2110	08010440	sha256_block0	Input data block
		…	…	…	…	
		1f	211f	0801047c	sha256_block15	
		20	2120	08010480	sha256_digest0	Output message digest
		…	…	…	…	
		27	2127	0801049c	sha256_digest7	
	02 SHA-512	00	2200	08010800	sha512_name0	"sha2"
		01	2201	08010804	sha512_name1	"-512"

seg	core	reg	reg addr	EIM addr	name	description
		02	2202	08010808	sha512_version	"0.80"
		08	2208	08010820	sha512_ctrl	bit 0 = init, bit 1 = next
		09	2209	08010824	sha512_status	bit 0 = ready, bit 1 = valid
		10	2210	08010840	sha512_block0	Input data block
		…	…	…	…	
		2f	222f	0801088c	sha512_block31	
		40	2240	08010900	sha512_digest0	Output message digest
		…	…	…	…	
		47	2247	0801091c	sha512_digest15	
02 TRNG	00 TRNG control	00	4000	08020000	trng_name0	"trng"
		01	4001	08020004	trng_name1	" "
		02	4002	08020008	trng_version	"0.50"
		10	4010	08020040	trng_ctrl	bit 0 = discard, bit 1 = test
		11	4011	08020044	trng_status	undefined
		12	4012	08020048	trng_debug_ctrl	3 bits: 1= avalanche, 2 = rosc, 3 = mixer, 4 = csprng
		13	4013	0802004c	trng_debug_delay	update frequency, in clock cycles
	05 Avalanche entropy source	00	4500	08021400	entropy1_name0	"extn"
		01	4501	08021404	entropy1_name1	"oise"
		02	4502	08021408	entropy1_version	"0.10"
		10	4510	08021440	entropy1_ctrl	bit 0 = enable
		11	4511	08021444	entropy1_status	bit 0 = valid
		20	4520	08021480	entropy1_entropy	Entropy data
		30	4530	080214c0	entropy1_delta	
	06 Ring Oscillator entropy source	00	4600	08021800	entropy2_name0	"rosc"
		01	4601	08021804	entropy2_name1	" ent"
		02	4602	08021808	entropy2_version	"0.10"
		10	4610	08021840	entropy2_ctrl	bit 0 = enable
		11	4611	08021844	entropy2_status	bit 0 = valid
		18	4618	08021860	entropy2_opa	

seg	core	reg	reg addr	EIM addr	name	description
		19	4619	08021864	entropy2_opb	
		20	4620	08021880	entropy2_entropy	Entropy data
		21	4621	08021884	entropy2_raw	
		22	4622	08021888	entropy2_rosc	
	0a TRNG Mixer	00	4a00	08022800	mixer_name0	undefined
		01	4a01	08022804	mixer_name1	undefined
		02	4a02	08022808	mixer_version	undefined
		10	4a10	08022840	mixer_ctrl	bit 0 = enable, bit 1 = restart
		11	4a11	08022844	mixer_status	undefined
		20	4a20	08022880	mixer_timeout	
	0b CSPRNG	00	4b00	08022c00	csprng_name0	"cspr"
		01	4b01	08022c04	csprng_name1	"ng "
		02	4b02	08022c08	csprng_version	"0.50"
		10	4b10	08022c40	csprng_ctrl	bit 0 = enable, bit 1 = seed
		11	4b11	08022c44	csprng_status	bit 0 = valid
		20	4b20	08022c80	csprng_random	Random data
		40	4b40	08022d00	csprng_nrounds	
		41	4b41	08022d04	csprng_nblocks_lo	
		42	4b42	08022d08	csprng_nblocks_hi	
03 Cipher	00 AES	00	6000	08030000	aes_name0	"aes "
		01	6001	08030004	aes_name1	" "
		02	6002	08030008	aes_version	"0.80"
		08	6008	08030020	aes_ctrl	
		09	6009	08030024	aes_status	
		0a	600a	08030028	aes_config	
		10	6010	08030040	aes_key0	
		…	…	…	…	
		17	6017	0803005c	aes_key7	
		20	6020	08030080	aes_block0	
		…	…	…	…	
		23	6023	0803008c	aes_block3	

seg	core	reg	reg addr	EIM addr	name	description
		30	6030	080300c0	aes_result0	
		…	…	…	…	
		33	6033	080300cc	aes_result3	
	01 Chacha	00	6100	08030400	chacha_name0	"chac"
		01	6101	08030404	chacha_name1	"ha "
		02	6102	08030408	chacha_version	"0.80"
		08	6108	08030420	chacha_ctrl	
		09	6109	08030424	chacha_status	
		0a	610a	08030428	chacha_keylen	
		0b	610b	0803042c	chacha_rounds	
		10	6110	08030440	chacha_key0	
		…	…	…	…	
		17	6117	0803045c	chacha_key7	
		20	6120	08030480	chacha_iv0	
		21	6121	08030484	chacha_iv1	
		40	6140	08030500	chacha_data_in0	
		…	…	…	…	
		4f	614f	0803053c	chacha_data_in15	
		80	6180	08030600	chacha_data_out0	
		…	…	…	…	
		8f	618f	0803063c	chacha_data_out15	
04	00	00	8000	08040000	modexp_name0	"mode"
		01	8001	08040004	modexp_name1	"xp "
		02	8002	08040008	modexp_version	"0.51"
		08	8008	08040020	modexp_ctrl	
		09	8009	08040024	modexp_status	
		13	8013	0804004c	modexp_delay	
		20	8020	08040080	modexp_modulus_length	
		21	8021	08040084	modexp_exponent_length	
		22	8022	08040088	modexp_length	
		30	8030	080400c0	modexp_modulus_ptr_rst	
		31	8031	080400c4	modexp_modulus_data	
		40	8040	08040100	modexp_exponent_ptr_rst	

seg	core	reg	reg addr	EIM addr	name	description
		41	8041	08040104	modexp_exponent_data	
		50	8050	08040140	modexp_message_ptr_rst	
		51	8051	08040144	modexp_message_data	
		60	8060	08040180	modexp_result_ptr_rst	
		61	8061	08040184	modexp_result_data	