Chapter 23 Crypto

23.1 Overview

Crypto is a hardware accelerator of encrypting or decrypting. It supports the most commonly used algorithm: DES/3DES, AES, SHA1, SHA256, MD5 and RSA.

The Crypto supports following features:

- Support AES 128/192/256 bits key mode, ECB/CBC/CTR chain mode, Slave/FIFO mode
- Support DES/3DES (ECB and CBC chain mode) , 3DES (EDE/ EEE key mode), Slave/FIFO mode
- Support SHA1/SHA256/MD5 (with hardware padding) HASH function, FIFO mode only
- Support 160 bit Pseudo Random Number Generator (PRNG)
- Support PKA 512/1024/2048 bit Exp Modulator
- Support up to 150M clock frequency

23.2 Block Diagram

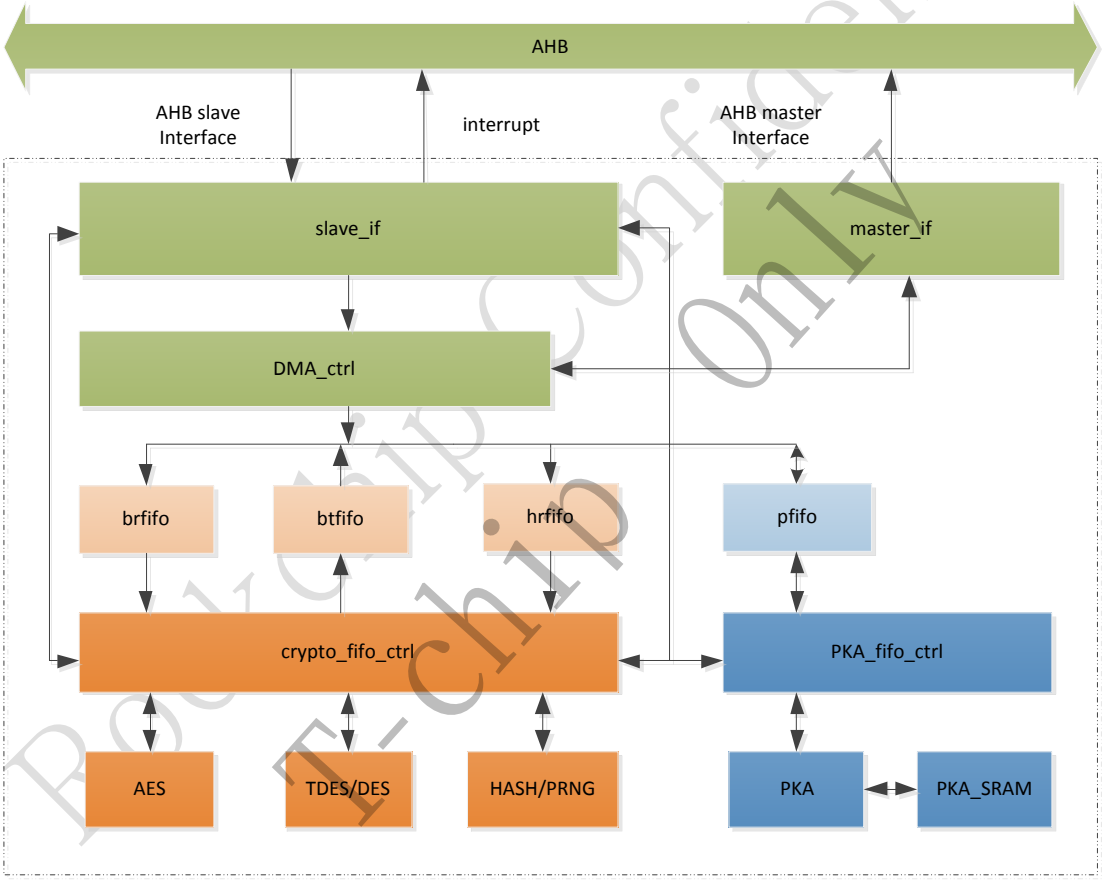

Fig. 23-1 Crypto Architecture

Figure above shows the architecture of Crypto.

Rockchip Confidential T-chip Only

23.3 Register description

23.3.1 Register Summary

Name	Offset	Size	Reset Value	Description
CRYPTO_INTSTS	0x0000	W	0x00000000	Interrupt Status Register
CRYPTO_INTENA	0x0004	W	0x00000000	Interrupt Set Register
CRYPTO_CTRL	0x0008	W	0x00000000	Control Register
CRYPTO_CONF	0x000c	W	0x00000000	
CRYPTO_BRDMAS	0x0010	W	0x00000000	Block Receiving DMA Start Address Register
CRYPTO_BTDMAS	0x0014	W	0x00000000	Block Transmiting DMA Start Address Register
CRYPTO_BRDMAL	0x0018	W	0x00000000	Block Receiving DMA Length Register
CRYPTO_HRDMAS	0x001c	W	0x00000000	Hash Receiving DMA Start Address Register
CRYPTO_HRDMAL	0x0020	W	0x00000000	Hash Receiving DMA Length Register
CRYPTO_AES_CTRL	0x0080	W	0x00000000	AES Control Register
CRYPTO_AES_STS	0x0084	W	0x00000000	Status Register
CRYPTO_AES_DIN_0	0x0088	W	0x00000000	AES Input Data 0 Register
CRYPTO_AES_DIN_1	0x008c	W	0x00000000	AES Input Data 1 Register
CRYPTO_AES_DIN_2	0x0090	W	0x00000000	AES Input Data 2 Register
CRYPTO_AES_DIN_3	0x0094	W	0x00000000	AES Input Data 3 Register
CRYPTO_AES_DOUT_0	0x0098	W	0x00000000	AES Output Data 0 Register
CRYPTO_AES_DOUT_1	0x009c	W	0x00000000	AES Output Data 1 Register
CRYPTO_AES_DOUT_2	0x00a0	W	0x00000000	AES Output Data 2 Register
CRYPTO_AES_DOUT_3	0x00a4	W	0x00000000	AES Output Data 3 Register
CRYPTO_AES_IV_0	0x00a8	W	0x00000000	AES IV data 0 Register
CRYPTO_AES_IV_1	0x00ac	W	0x00000000	AES IV data 1 Register
CRYPTO_AES_IV_2	0x00b0	W	0x00000000	AES IV data 2 Register
CRYPTO_AES_IV_3	0x00b4	W	0x00000000	AES IV data 3 Register
CRYPTO_AES_KEY_0	0x00b8	W	0x00000000	AES Key data 0 Register
CRYPTO_AES_KEY_1	0x00bc	W	0x00000000	AES Key data 1 Register
CRYPTO_AES_KEY_2	0x00c0	W	0x00000000	AES Key data 2 Register
CRYPTO_AES_KEY_3	0x00c4	W	0x00000000	AES Key data 3 Register
CRYPTO_AES_KEY_4	0x00c8	W	0x00000000	AES Key data 4 Register
CRYPTO_AES_KEY_5	0x00cc	W	0x00000000	AES Key data 5 Register
CRYPTO_AES_KEY_6	0x00d0	W	0x00000000	AES Key data 6 Register

Rockchip Confidential T-chip only

Name	Offset	Size	Reset Value	Description
CRYPTO_AES_KEY_7	0x00d4	W	0x00000000	AES Key data 7 Register
CRYPTO_AES_CNT_0	0x00d8	W	0x00000000	AES Input Counter 0 Register
CRYPTO_AES_CNT_1	0x00dc	W	0x00000000	AES Input Counter 1 Register
CRYPTO_AES_CNT_2	0x00e0	W	0x00000000	AES Input Counter 2 Register
CRYPTO_AES_CNT_3	0x00e4	W	0x00000000	AES Input Counter 3 Register
CRYPTO_TDES_CTRL	0x0100	W	0x00000000	TDES Control Register
CRYPTO_TDES_STS	0x0104	W	0x00000000	Status Register
CRYPTO_TDES_DIN_0	0x0108	W	0x00000000	TDES Input Data 0 Register
CRYPTO_TDES_DIN_1	0x010c	W	0x00000000	TDES Input Data 1 Register
CRYPTO_TDES_DOUT_0	0x0110	W	0x00000000	TDES Output Data 0 Register
CRYPTO_TDES_DOUT_1	0x0114	W	0x00000000	TDES Output Data 1 Register
CRYPTO_TDES_IV_0	0x0118	W	0x00000000	TDES IV data 0 Register
CRYPTO_TDES_IV_1	0x011c	W	0x00000000	TDES IV data 1 Register
CRYPTO_TDES_KEY1_0	0x0120	W	0x00000000	TDES Key1 data 1 Register
CRYPTO_TDES_KEY1_1	0x0124	W	0x00000000	TDES Key1 data 1 Register
CRYPTO_TDES_KEY2_0	0x0128	W	0x00000000	TDES Key2 data 0 Register
CRYPTO_TDES_KEY2_1	0x012c	W	0x00000000	TDES Key2 data 1 Register
CRYPTO_TDES_KEY3_0	0x0130	W	0x00000000	TDES Key3 data 0 Register
CRYPTO_TDES_KEY3_1	0x0134	W	0x00000000	TDES Key3 data 1 Register
CRYPTO_HASH_CTRL	0x0180	W	0x00000000	Hash Control Register
CRYPTO_HASH_STS	0x0184	W	0x00000000	Hash Status Register
CRYPTO_HASH_MSG_LEN	0x0188	W	0x00000000	Hash Message Len
CRYPTO_HASH_DOUT_0	0x018c	W	0x00000000	Hash Result Register 0
CRYPTO_HASH_DOUT_1	0x0190	W	0x00000000	Hash Result Register 1
CRYPTO_HASH_DOUT_2	0x0194	W	0x00000000	Hash Result Register 2
CRYPTO_HASH_DOUT_3	0x0198	W	0x00000000	Hash Result Register 3
CRYPTO_HASH_DOUT_4	0x019c	W	0x00000000	Hash Result Register 4

Rockchip Confidential
Only for Fuzhou Rockchip

Name	Offset	Size	Reset Value	Description
CRYPTO_HASH_DOUT_5	0x01a0	W	0x00000000	Hash Result Register 4
CRYPTO_HASH_DOUT_6	0x01a4	W	0x00000000	Hash Result Register 6
CRYPTO_HASH_DOUT_7	0x01a8	W	0x00000000	Hash Result Register 7
CRYPTO_HASH_SEED_0	0x01ac	W	0x00000000	PRNG Seed/HMAC Key Register 0
CRYPTO_HASH_SEED_1	0x01b0	W	0x00000000	PRNG Seed/HMAC Key Register 1
CRYPTO_HASH_SEED_2	0x01b4	W	0x00000000	PRNG Seed/HMAC Key Register 2
CRYPTO_HASH_SEED_3	0x01b8	W	0x00000000	PRNG Seed/HMAC Key Register 3
CRYPTO_HASH_SEED_4	0x01bc	W	0x00000000	PRNG Seed/HMAC Key Register 4
CRYPTO_TRNG_CTRL	0x0200	W	0x00000000	TRNG Control
CRYPTO_TRNG_DOUT_0	0x0204	W	0x00000000	TRNG Output Data 0
CRYPTO_TRNG_DOUT_1	0x0208	W	0x00000000	TRNG Output Data 1
CRYPTO_TRNG_DOUT_2	0x020c	W	0x00000000	TRNG Output Data 2
CRYPTO_TRNG_DOUT_3	0x0210	W	0x00000000	TRNG Output Data 3
CRYPTO_TRNG_DOUT_4	0x0214	W	0x00000000	TRNG Output Data 4
CRYPTO_TRNG_DOUT_5	0x0218	W	0x00000000	TRNG Output Data 5
CRYPTO_TRNG_DOUT_6	0x021c	W	0x00000000	TRNG Output Data 6
CRYPTO_TRNG_DOUT_7	0x0220	W	0x00000000	TRNG Output Data 7
CRYPTO_PKA_CTRL	0x0280	W	0x00000000	PKA Control Register
CRYPTO_PKA_M	0x0400	W	0x00000000	
CRYPTO_PKA_C	0x0500	W	0x00000000	
CRYPTO_PKA_N	0x0600	W	0x00000000	
CRYPTO_PKA_E	0x0700	W	0x00000000	

*Notes: Size : **B** - Byte (8 bits) access, **HW** - Half WORD (16 bits) access, **W** -WORD (32 bits) access*

23.3.2 Detail Register Description

CRYPTO_INTSTS

Rockchip Confidential
It-chip only

Address: Operational Base + offset (0x0000)
Interrupt Status Register

Bit	Attr	Reset Value	Description
31:6	RO	0x0	reserved
5	RW	0x0	PKA_DONE_INT PKA Done Interrupt
4	W1C	0x0	HASH_DONE_INT Hash Done Interrupt
3	W1C	0x0	HRDMA_ERR_INT Specifies the interrupt of hash receiving DMA Error
2	W1C	0x0	HRDMA_DONE_INT Specifies the interrupt of hash receiving DMA DONE
1	W1C	0x0	BCDMA_ERR_INT Specifies the interrupt of block cipher Error
0	W1C	0x0	BCDMA_DONE_INT Specifies the interrupt of block cipher DONE

CRYPTO_INTENA
Address: Operational Base + offset (0x0004)
Interrupt Set Register

Bit	Attr	Reset Value	Description
31:6	RO	0x0	reserved
5	RW	0x0	PKA_DONE_ENA Set the interrupt Enable of PKA done 1'b1: enable 1'b0: disable
4	RW	0x0	HASH_DONE_ENA Set the interrupt Enable of hash done 1'b1: enable 1'b0: disable
3	RW	0x0	HRDMA_ERR_ENA Set the interrupt Enable of hash receiving DMA Error 1'b1: enable 1'b0: disable

Rockchip Confidential
T-Chip Only

Bit	Attr	Reset Value	Description
2	RW	0x0	HRDMA_DONE_ENA Set the interrupt Enable of hash receiving DMA DONE 1'b1: enable 1'b0: disable
1	RW	0x0	BCDMA_ERR_ENA Set the interrupt Enable of block cipher DMA Error 1'b1: enable 1'b0: disable
0	RW	0x0	BCDMA_DONE_ENA Set the interrupt Enable of block cipher DMA DONE 1'b1: enable 1'b0: disable

CRYPTO_CTRL
Address: Operational Base + offset (0x0008)
Control Register

Bit	Attr	Reset Value	Description
31:16	RW	0x0000	Write_Mask
15:10	RO	0x0	reserved
9	RW	0x0	TRNG_FLUSH FLUSH TRNG Software write 1 to start. When finishes, the core will clear it.
8	R/WSC	0x0	TRNG_START Start TRNG Software write 1 to start. When finishes, the core will clear it.
7	R/WSC	0x0	PKA_FLUSH Software write 1 to start Flush Process.The process will clear BRFIFO, BTFIFO, and state machine. Then Software should write 0 to end FLUSH Process
6	RW	0x0	HASH_FLUSH Software write 1 to start Flush Process.The process will clear BRFIFO, BTFIFO, and state machine. Then Software should write 0 to end FLUSH Process

Rockchip Confidential
T-chip Only

Bit	Attr	Reset Value	Description
5	RW	0x0	BLOCK_FLUSH Software write 1 to start Flush Process.The process will clear BRFIFO, BTFIFO, and state machine. Then Software should write 0 to end FLUSH Process. It must last for at least 20 cycles to clean registers and FSM
4	R/WSC	0x0	PKA_START Starts/initializes PKA Software write 1 to start. When finishes, the core will clear it.
3	R/WSC	0x0	HASH_START Starts/initializes HASH/PRNG/HMAC Software write 1 to start. When finishes, the core will clear it.
2	R/WSC	0x0	BLOCK_START Starts/initializes Block Cipher Software write 1 to start. When finishes, the core will clear it.
1	R/WSC	0x0	TDES_START Starts/initializes TDES Software write 1 to start. When finishes, the core will clear it.
0	R/WSC	0x0	AES_START Starts/initializes AES Software write 1 to start. When finishes, the core will clear it. Software can also write 0 to clear it.

CRYPTO_CONF
Address: Operational Base + offset (0x000c)

Bit	Attr	Reset Value	Description
31:9	RO	0x0	reserved
8	RW	0x0	HR_ADDR_MODE Hash Receive DMA Address Mode 1'b1: fix 1'b0: increment
7	RW	0x0	BT_ADDR_MODE Block Transmit DMA Address Mode 1'b1: fix 1'b0: increment
6	RW	0x0	BR_ADDR_MODE Block Receive DMA Address Mode 1'b1: fix 1'b0: increment

Rockchip Confidential T-chip Only

Bit	Attr	Reset Value	Description
5	RW	0x0	Byteswap_HRFIFO If this bit is high, then the data read from the bus is byte-swapped in a word boundary. If this bit is low (default), then the data is handed over to the FIFO without byte-swap. For little endian bus, this bit should be 1'b1.
4	RW	0x0	Byteswap_BTFIFO If this bit is high, then the data read from the bus is byte-swapped in a word boundary. If this bit is low (default), then the data is handed over to the FIFO without byte-swap. For little endian bus, this bit should be 1'b1.
3	RW	0x0	Byteswap_BRFIFO If this bit is high, then the data read from the bus is byte-swapped in a word boundary. If this bit is low (default), then the data is handed over to the FIFO without byte-swap. For little endian bus, this bit should be 1'b1.
2	RW	0x0	DESSEL Specifies the Destination block cipher of FIFO. AES(=0)/DES(=1)
1:0	RW	0x0	HASHINSEL Specifies the following Data from independent source (0) Data from block cipher input (1) Data from block cipher output (2) Reserved (3)

CRYPTO_BRDMAS
Address: Operational Base + offset (0x0010)
Block Receiving DMA Start Address Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	STARTADDR Specifies the Start Address of DMA The address should be aligned by 32-bit.

CRYPTO_BTDMAS
Address: Operational Base + offset (0x0014)
Block Transmiting DMA Start Address Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	STARTADDR Specifies the Start Address of DMA The address needs to be aligned by 32-bit.

CRYPTO_BRDMAL

Rockchip Confidential T-Chip Only

Address: Operational Base + offset (0x0018)
Block Receiving DMA Length Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	LENGTH Specifies the Block length of DMA. The length unit is WORD.

CRYPTO_HRDMAS
Address: Operational Base + offset (0x001c)
Hash Receiving DMA Start Address Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	STARTADDR Specifies the Start Address of DMA The address needs to be aligned by 32-bit.

CRYPTO_HRDMAL
Address: Operational Base + offset (0x0020)
Hash Receiving DMA Length Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	LENGTH Specifies the Block length of DMA. The length unit is BYTE.

CRYPTO_AES_CTRL
Address: Operational Base + offset (0x0080)
AES Control Register

Bit	Attr	Reset Value	Description
31:12	RO	0x0	reserved
11	RW	0x0	AES_ByteSwap_CNT Change the Big-endian and Little-endian by swapping the byte oder. 0 = Disables Counter data byte swap 1 = Enables Counter data byte swap
10	RW	0x0	AES_ByteSwap_Key Change the Big-endian and Little-endian by swapping the byte oder. 0 = Disables Key byte swap 1 = Enables Key byte swap
9	RW	0x0	AES_ByteSwap_IV Change the Big-endian and Little-endian by swapping the byte oder. 0 = Disables Initial value byte swap 1 = Enables Initial value byte swap

Rockchip Confidential T-chip only

Bit	Attr	Reset Value	Description
8	RW	0x0	AES_ByteSwap_DO Change the Big-endian and Little-endian by swapping the byte oder. 0 = Disables Output data byte swap 1 = Enables Output data byte swap
7	RW	0x0	AES_ByteSwap_DI Change the Big-endian and Little-endian by swapping the byte oder. 0 = Disables Input data byte swap 1 = Enables Input data byte swap
6	RW	0x0	AES_KeyChange Specifies the AES key change mode selection signal. When the bit is asserted, it will not do key-expansion function to calculate new sub-key. So it is a faster way, when several times of calculation use the same key. But if the keys are different, asserting this bit will have the wrong result. 0 = Key is not changed 1 = Key is changed
5:4	RW	0x0	AES_ChainMode Specifies AES chain mode selection 00 = ECB mode 01 = CBC mode 10 = CTR mode
3:2	RW	0x0	AES_KeySize Specifies the AES key size selection signal 00 : 128-bit key 01 : 192-bit key 10 : 256-bit key
1	RW	0x0	AES_FifoMode Specify AES Fifo Mode 1'b0: Slave mode 1'b1: fifo mode
0	RW	0x0	AES_Enc Specifies the Encryption/ Decryption mode selection signal 0 : Encryption 1 : Decryption

CRYPTO_AES_STS

Address: Operational Base + offset (0x0084)

Status Register

Bit	Attr	Reset Value	Description

Rockchip Confidential T-chip Only

Bit	Attr	Reset Value	Description
31:1	RO	0x0	reserved
0	RW	0x0	AES_DONE When AES finish, it will be HIGH, And it will not be LOW until it restart . 1: done 0: not done

CRYPTO_AES_DIN_0
Address: Operational Base + offset (0x0088)
AES Input Data 0 Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	AES_DIN_0 Specifies AES Input data [127:96].

CRYPTO_AES_DIN_1
Address: Operational Base + offset (0x008c)
AES Input Data 1 Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	AES_DIN_1 Specifies AES Input data [95:64].

CRYPTO_AES_DIN_2
Address: Operational Base + offset (0x0090)
AES Input Data 2 Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	AES_DIN_2 Specifies AES Input data [63:32]

CRYPTO_AES_DIN_3
Address: Operational Base + offset (0x0094)
AES Input Data 3 Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	AES_DIN_3 Specifies AES Input data [31:0]

CRYPTO_AES_DOUT_0
Address: Operational Base + offset (0x0098)
AES Output Data 0 Register

Bit	Attr	Reset Value	Description

Rockchip Confidential
T-chip Only

Bit	Attr	Reset Value	Description
31:0	RO	0x00000000	AES_DOUT_0 Specifies AES Output data [127:96].

CRYPTO_AES_DOUT_1
Address: Operational Base + offset (0x009c)
AES Output Data 1 Register

Bit	Attr	Reset Value	Description
31:0	RO	0x00000000	AES_DOUT_1 Specifies the Output data [95:64].

CRYPTO_AES_DOUT_2
Address: Operational Base + offset (0x00a0)
AES Output Data 2 Register

Bit	Attr	Reset Value	Description
31:0	RO	0x00000000	AES_DOUT_2 Specifies AES Output data [63:32].

CRYPTO_AES_DOUT_3
Address: Operational Base + offset (0x00a4)
AES Output Data 3 Register

Bit	Attr	Reset Value	Description
31:0	RO	0x00000000	AES_DOUT_3 Specifies AES Output data [31:0].

CRYPTO_AES_IV_0
Address: Operational Base + offset (0x00a8)
AES IV data 0 Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	AES_IV_0 Specifies AES Initialization vector [127:96]

CRYPTO_AES_IV_1
Address: Operational Base + offset (0x00ac)
AES IV data 1 Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	AES_IV_1 Specifies AES Initialization vector [95:64]

Rockchip Confidential
T-Chip Only

CRYPTO_AES_IV_2
Address: Operational Base + offset (0x00b0)
AES IV data 2 Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	AES_IV_2 Specifies AES Initialization vector [63:32]

CRYPTO_AES_IV_3
Address: Operational Base + offset (0x00b4)
AES IV data 3 Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	AES_IV_3 Specifies AES Initialization vector [31:0]

CRYPTO_AES_KEY_0
Address: Operational Base + offset (0x00b8)
AES Key data 0 Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	AES_KEY_0 Specifies AES key data [255:224]

CRYPTO_AES_KEY_1
Address: Operational Base + offset (0x00bc)
AES Key data 1 Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	AES_KEY_1 Specifies AES key data [223:192]

CRYPTO_AES_KEY_2
Address: Operational Base + offset (0x00c0)
AES Key data 2 Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	AES_KEY_2 Specifies AES key data [191:160]

CRYPTO_AES_KEY_3
Address: Operational Base + offset (0x00c4)
AES Key data 3 Register

Bit	Attr	Reset Value	Description

Rockchip Confidential
T-chip Only

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	AES_KEY_3 Specifies AES key data [159:128]

CRYPTO_AES_KEY_4
Address: Operational Base + offset (0x00c8)
AES Key data 4 Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	AES_KEY_4 Specifies AES key data [127:96]

CRYPTO_AES_KEY_5
Address: Operational Base + offset (0x00cc)
AES Key data 5 Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	AES_KEY_5 Specifies the key data [95:64]

CRYPTO_AES_KEY_6
Address: Operational Base + offset (0x00d0)
AES Key data 6 Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	AES_KEY_6 Specifies AES key data [63:32]

CRYPTO_AES_KEY_7
Address: Operational Base + offset (0x00d4)
AES Key data 7 Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	AES_KEY_7 Specifies the key data [31:0]

CRYPTO_AES_CNT_0
Address: Operational Base + offset (0x00d8)
AES Input Counter 0 Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	AES_CNT_0 Specifies AES Input Counter [127:96].

Rockchip Confidential
T-Chip Only

CRYPTO_AES_CNT_1
Address: Operational Base + offset (0x00dc)
AES Input Counter 1 Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	AES_CNT_1 Specifies AES Input Counter [95:64].

CRYPTO_AES_CNT_2
Address: Operational Base + offset (0x00e0)
AES Input Counter 2 Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	AES_CNT_2 Specifies AES Input Counter[63:32]

CRYPTO_AES_CNT_3
Address: Operational Base + offset (0x00e4)
AES Input Counter 3 Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	AES_CNT_3 Specifies AES Input Counter [31:0]

CRYPTO_TDES_CTRL
Address: Operational Base + offset (0x0100)
TDES Control Register

Bit	Attr	Reset Value	Description
31:9	RO	0x0	reserved
8	RW	0x0	TDES_ByteSwap_Key 0 = Disables Key byte swap 1 = Enables Key byte swap
7	RW	0x0	TDES_ByteSwap_IV 0 = Disables Initial value byte swap 1 = Enables Initial value byte swap
6	RW	0x0	TDES_ByteSwap_DO 0 = Disables Output data byte swap 1 = Enables Output data byte swap
5	RW	0x0	TDES_ByteSwap_DI 0 = Disables Input data byte swap 1 = Enables Input data byte swap
4	RW	0x0	TDES_ChainMode Specifies TDES chain mode selection 0 : ECB mode 1 : CBC mode

Rockchip Confidential T-chip only

Bit	Attr	Reset Value	Description
3	RW	0x0	TDES_EEE Specifies the TDES key mode selection 1'b0 : EDE 1'b1 : EEE
2	RW	0x0	TDES_Select Specify DES or TDES cipher 1'b0 : DES 1'b1 : TDES
1	RW	0x0	TDES_FifoMode Specify TDES Fifo Mode 1'b0: Slave mode 1'b1: Fifo mode
0	RW	0x0	TDES_Enc Specifies the Encryption/ Decryption mode selection signal 0 : Encryption 1 : Decryption

CRYPTO_TDES_STS
Address: Operational Base + offset (0x0104)
Status Register

Bit	Attr	Reset Value	Description
31:1	RO	0x0	reserved
0	RW	0x0	TDES_DONE When DES/TDES finishes, it will be HIGH, And it will not be LOW until it restart . 1: done 0: not done

CRYPTO_TDES_DIN_0
Address: Operational Base + offset (0x0108)
TDES Input Data 0 Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	TDES_DIN_0 Specifies TDES Input data [63:32].

CRYPTO_TDES_DIN_1
Address: Operational Base + offset (0x010c)
TDES Input Data 1 Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	TDES_DIN_1 Specifies TDES Input data [31:0].

Rockchip Confidential
Rockchip Only

CRYPTO_TDES_DOUT_0
Address: Operational Base + offset (0x0110)
TDES Output Data 0 Register

Bit	Attr	Reset Value	Description
31:0	RO	0x00000000	TDES_DOUT_0 Specifies TDES Output data [63:32].

CRYPTO_TDES_DOUT_1
Address: Operational Base + offset (0x0114)
TDES Output Data 1 Register

Bit	Attr	Reset Value	Description
31:0	RO	0x00000000	TDES_DOUT_1 Specifies TDES Output data [31:0].

CRYPTO_TDES_IV_0
Address: Operational Base + offset (0x0118)
TDES IV data 0 Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	TDES_IV_0 Specifies TDES Initialization vector [63:32]

CRYPTO_TDES_IV_1
Address: Operational Base + offset (0x011c)
TDES IV data 1 Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	TDES_IV_1 Specifies TDES Initialization vector [31:0]

CRYPTO_TDES_KEY1_0
Address: Operational Base + offset (0x0120)
TDES Key1 data 1 Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	TDES_KEY1_0 Specifies TDES key1 data [63:32]

CRYPTO_TDES_KEY1_1
Address: Operational Base + offset (0x0124)
TDES Key1 data 1 Register

Bit	Attr	Reset Value	Description

Rockchip Confidential
T-chip Only

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	TDES_KEY1_1 Specifies TDES key1 data [31:0]

CRYPTO_TDES_KEY2_0
Address: Operational Base + offset (0x0128)
TDES Key2 data 0 Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	TDES_KEY2_0 Specifies TDES key2 data [63:32]

CRYPTO_TDES_KEY2_1
Address: Operational Base + offset (0x012c)
TDES Key2 data 1 Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	TDES_KEY_1 Specifies TDES key data [31:0]

CRYPTO_TDES_KEY3_0
Address: Operational Base + offset (0x0130)
TDES Key3 data 0 Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	TDES_KEY3_0 Specifies TDES key3 data [63:32]

CRYPTO_TDES_KEY3_1
Address: Operational Base + offset (0x0134)
TDES Key3 data 1 Register

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	AES_KEY3_1 Specifies TDES key3 data [31:0]

CRYPTO_HASH_CTRL
Address: Operational Base + offset (0x0180)
Hash Control Register

Bit	Attr	Reset Value	Description
31:4	RO	0x0	reserved

Rockchip Confidential
T-Chip Only

Bit	Attr	Reset Value	Description
3	RW	0x0	HASH_SWAP_DO Specifies the Byte swap of data output (hash result) 0 = Does not swap (default) 1 = Swap
2	RW	0x0	HASH_SWAP_DI Specifies the Byte swap of data input. 0 = Does not swap (default) 1 = Swap
1:0	RW	0x0	Engine_Selection 2'b00: SHA1_HASH 2'b01: MD5_HASH 2'b10: SHA256_HASH 2'b11: PRNG

CRYPTO_HASH_STS
Address: Operational Base + offset (0x0184)
Hash Status Register

Bit	Attr	Reset Value	Description
31:1	RO	0x0	reserved
0	RW	0x0	HASH_DONE Hash Done Signal When HASH finishes, it will be HIGH, And it will not be LOW until it restart 1'b1 : done 1'b0 : not done

CRYPTO_HASH_MSG_LEN
Address: Operational Base + offset (0x0188)
Hash Message Len

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	Msg_size Hash total byte.

CRYPTO_HASH_DOUT_0
Address: Operational Base + offset (0x018c)
Hash Result Register 0

Bit	Attr	Reset Value	Description
31:0	RO	0x00000000	HASH_RESULT_0 Specifies the HASH Result [159:128]

CRYPTO_HASH_DOUT_1
Address: Operational Base + offset (0x0190)
Hash Result Register 1

Rockchip confidential
T-chip only

Bit	Attr	Reset Value	Description
31:0	RO	0x00000000	HASH_RESULT_1 Specifies the HASH Result [127:96]

CRYPTO_HASH_DOUT_2
Address: Operational Base + offset (0x0194)
Hash Result Register 2

Bit	Attr	Reset Value	Description
31:0	RO	0x00000000	HASH_RESULT_2 Specifies the HASH Result [95:64]

CRYPTO_HASH_DOUT_3
Address: Operational Base + offset (0x0198)
Hash Result Register 3

Bit	Attr	Reset Value	Description
31:0	RO	0x00000000	HASH_RESULT_3 Specifies the HASH Result [63:32]

CRYPTO_HASH_DOUT_4
Address: Operational Base + offset (0x019c)
Hash Result Register 4

Bit	Attr	Reset Value	Description
31:0	RO	0x00000000	HASH_RESULT_4 Specifies the HASH Result [31:0]

CRYPTO_HASH_DOUT_5
Address: Operational Base + offset (0x01a0)
Hash Result Register 4

Bit	Attr	Reset Value	Description
31:0	RO	0x00000000	HASH_RESULT_5 Specifies the HASH Result [31:0]

CRYPTO_HASH_DOUT_6
Address: Operational Base + offset (0x01a4)
Hash Result Register 6

Bit	Attr	Reset Value	Description
31:0	RO	0x00000000	HASH_RESULT_6 Specifies the HASH Result [31:0]

Rockchip Confidential
T-Chip Only

CRYPTO_HASH_DOUT_7
Address: Operational Base + offset (0x01a8)
Hash Result Register 7

Bit	Attr	Reset Value	Description
31:0	RO	0x00000000	HASH_RESULT_7 Specifies the HASH Result [31:0]

CRYPTO_HASH_SEED_0
Address: Operational Base + offset (0x01ac)
PRNG Seed/HMAC Key Register 0

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	HASH_SEED_0 Specifies PRNG Seed/HMAC Key buffer [159:128]

CRYPTO_HASH_SEED_1
Address: Operational Base + offset (0x01b0)
PRNG Seed/HMAC Key Register 1

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	HASH_SEED_1 Specifies PRNG Seed/HMAC Key buffer [127:96]

CRYPTO_HASH_SEED_2
Address: Operational Base + offset (0x01b4)
PRNG Seed/HMAC Key Register 2

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	HASH_SEED_2 Specifies PRNG Seed/HMAC Key buffer [95:64]

CRYPTO_HASH_SEED_3
Address: Operational Base + offset (0x01b8)
PRNG Seed/HMAC Key Register 3

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	HASH_SEED_3 Specifies PRNG Seed/HMAC Key buffer [63:32]

CRYPTO_HASH_SEED_4
Address: Operational Base + offset (0x01bc)

Rockchip Confidential T-Chip Only

PRNG Seed/HMAC Key Register 4

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	HASH_SEED_4 Specifies PRNG Seed/HMAC Key buffer [31:0]

CRYPTO_TRNG_CTRL

Address: Operational Base + offset (0x0200)

TRNG Control

Bit	Attr	Reset Value	Description
31:17	RO	0x0	reserved
16	RW	0x0	osc_enable osc_ring enable It controll the running of osc_ring. And it is indepent of clock and flush signal. This mean that it can run even when clock is gating or flush is asserted as long as osc_enable is asserted. Before it is used to get TRNG result , please run osc_ring first to get enough entropy. 1'b1: Enable ; 1'b0: Disable ;
15:0	RW	0x0000	period sample period TRNG use clock_crypto to sample ring osc output, this parameter is specify how many cycles to generate 1 bit random data.

CRYPTO_TRNG_DOUT_0

Address: Operational Base + offset (0x0204)

TRNG Output Data 0

Bit	Attr	Reset Value	Description
31:0	RO	0x00000000	TRNG_DOUT_0

CRYPTO_TRNG_DOUT_1

Address: Operational Base + offset (0x0208)

TRNG Output Data 1

Bit	Attr	Reset Value	Description
31:0	RO	0x00000000	TRNG_DOUT_1

CRYPTO_TRNG_DOUT_2

Address: Operational Base + offset (0x020c)

TRNG Output Data 2

Bit	Attr	Reset Value	Description

Rockchip Confidential
T-chip Only

Bit	Attr	Reset Value	Description
31:0	RO	0x00000000	TRNG_DOUT_2

CRYPTO_TRNG_DOUT_3
Address: Operational Base + offset (0x0210)
TRNG Output Data 3

Bit	Attr	Reset Value	Description
31:0	RO	0x00000000	TRNG_DOUT_3

CRYPTO_TRNG_DOUT_4
Address: Operational Base + offset (0x0214)
TRNG Output Data 4

Bit	Attr	Reset Value	Description
31:0	RO	0x00000000	TRNG_DOUT_4

CRYPTO_TRNG_DOUT_5
Address: Operational Base + offset (0x0218)
TRNG Output Data 5

Bit	Attr	Reset Value	Description
31:0	RO	0x00000000	TRNG_DOUT_5

CRYPTO_TRNG_DOUT_6
Address: Operational Base + offset (0x021c)
TRNG Output Data 6

Bit	Attr	Reset Value	Description
31:0	RO	0x00000000	TRNG_DOUT_6

CRYPTO_TRNG_DOUT_7
Address: Operational Base + offset (0x0220)
TRNG Output Data 7

Bit	Attr	Reset Value	Description
31:0	RO	0x00000000	TRNG_DOUT_7

CRYPTO_PKA_CTRL
Address: Operational Base + offset (0x0280)
PKA Control Register

Bit	Attr	Reset Value	Description
31:2	RO	0x0	reserved

Rockchip Confidential
T-chip Only

Bit	Attr	Reset Value	Description
1:0	RW	0x0	block_size PKA Size It specifies the bits of N in PKA calculation. 2'b00: 512 bit 2'b01: 1024 bit 2'b10: 2048 bit

CRYPTO_PKA_M
Address: Operational Base + offset (0x0400)

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	m PKA input or output data. PKA result = (M ^ E) mod N. When it finishes, the result data is in M position. Start from PKA_M base address, and may contain 512/1024/2048 bits data.

CRYPTO_PKA_C
Address: Operational Base + offset (0x0500)

Bit	Attr	Reset Value	Description
31:1	RO	0x0	reserved
0	RW	0x0	c PKA pre-calculate data, C = 2 ^(2n+2) mod N

CRYPTO_PKA_N
Address: Operational Base + offset (0x0600)

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	n PKA modular

CRYPTO_PKA_E
Address: Operational Base + offset (0x0700)

Bit	Attr	Reset Value	Description
31:0	RW	0x00000000	e PKA exponent.

Rockchip Confidential
T-chip Only

23.4 Application Note

23.4.1 Reset a port

CRU_SOFTRST3_CON. crypto_srstn_req is used to do a soft reset to crypto . Please refer to "Chapter CRU" for more details.

23.4.2 Overall Performance

Use CLKSEL24_CON.crypto_div_con to select crypto frequency: $F_{crypto} = F_{aclk} / (div + 1)$. Make sure F_{crypto} do not exceed 150M.
The performance of crypto FIFO mode is list below.

algorithm	cycle	block size	frequency	throughput rate
DES	17	64 bit	100M	376 M bps
TDES	51	64 bit	100M	125 M bps
AES	11/13/15	128 bit	100M	1160/984/853Mbps
SHA-1	81	512 bit	100M	632 Mbps
MD5	65	512 bit	100M	787 Mbps

23.4.3 Usage

1. Symmetric algorithm

DES/3DES, AES are symmetric algorithms. There are two ways of using these algorithms: Slave mode and FIFO mode.

In Slave mode, you can calculate 1 block size of data by starting the engine. Take AES-128 for example, you should

- Program Input 128 bit Data to AES_DIN_0~AES_DIN_3
- Program Input 128 bit Key to AES_KEY_0~AES_KEY_3
- Program control mode to AES_CTRL to run in different mode
- Program CTRL.AES_START to run
- wait AES_STS.DONE High
- Read AES_DOUT_0 ~ AES_DOUT_3 to get result.

In FIFO mode,

- Program the source address to BRDMAS, the destination address to BTDMAS, program the length in word unit to BRDMAL;
- Program Input 128 bit Key to AES_KEY_0~AES_KEY_3;
- Program control mode to AES_CTRL to run in different mode;
- Program INTENA to enable interrupt;
- Program CTRL.BLOCK_START to start;
- wait interrupt asserted;
- Program INTSTS to clear interrupt status;
- Read the destination address which BTDMA points to.

FIFO mode get much higher throughput rate.

2. HASH

HASH is used to get digest of data. Only support FIFO mode.

There are three source: (1) hr_fifo; (2) br_fifo; (3) bt_fifo.

Rockchip Confidential
T-chip only

Take hr_fifo for example

(1) Program CTRL.HASH_FLUSH 1'b1 to clear, wait several cycle (>= 10 cycles) , and Program CTRL.HASH_FLUSH 1'b0

(2) Program data source address to HRDMAS, program 1 time data length in word unit to HRDMAL, program total length in byte unit to HASH_MSG_LEN

(3) Program HASH_CTRL to choose algorithm, for example SHA-256

(4) Program INTENA to enable interrupt;

(5) Program CTRL.HASH_START 1'b1 to start;

(6) Wait interrupt asserted; Only if HRDMAL length meets can this interrupt be asserted

(7) If you have another section of data to hash, then go to (2), HASH_MSG_LEN need not to be programmed;

else go to (8)

(8) wait HASH_STS.done asserted. Only if Hash_MSG_LEN meet can this bit status register asserted.

(9) Read HASH_DOUT_0 – HASH_DOUT_7 to get result.

3. Asymmetric Algorithm

Support 512/1024/2048 bit RSA calculation. It provide the big number calculation. Result = M^E mod N

Program CTRL.PKA_FLUSH 1'b1 to flush RSA module;

Wait CTRL.PKA_FLUSH to be LOW. It is self-cleared;

Program input_data(M) to PKA_M; Program pre_caculated C to PKA_C; Program Key(N) to PKA_N; Program Key(E) to PKA_E. C = $2^{(2n+2)}$ mod N. n is the required bit of N. For example 2048 bit N, n = 2048;

Program PKA_CTRL to select RSA size: 512/1024/2048

Program INTENA to enable interrupt;

Program CTRL.PKA_START to start;

Wait interrupt asserted.

Read PKA_M to get results.

Rockchip Confidential
T-chip only