

#### Welcome to E-XFL.COM

#### What is "Embedded - Microcontrollers"?

"Embedded - Microcontrollers" refer to small, integrated circuits designed to perform specific tasks within larger systems. These microcontrollers are essentially compact computers on a single chip, containing a processor core, memory, and programmable input/output peripherals. They are called "embedded" because they are embedded within electronic devices to control various functions, rather than serving as standalone computers. Microcontrollers are crucial in modern electronics, providing the intelligence and control needed for a wide range of applications.

#### Applications of "<u>Embedded -</u> <u>Microcontrollers</u>"

#### Details

E·XFI

Product Status	Active
Core Processor	ARM® Cortex®-M4F
Core Size	32-Bit Single-Core
Speed	120MHz
Connectivity	EBI/EMI, I <sup>2</sup> C, IrDA, LINbus, MMC/SD, QSPI, SPI, UART/USART, USB
Peripherals	Brown-out Detect/Reset, DMA, I <sup>2</sup> S, POR, PWM
Number of I/O	81
Program Memory Size	512KB (512K x 8)
Program Memory Type	FLASH
EEPROM Size	-
RAM Size	192К х 8
Voltage - Supply (Vcc/Vdd)	1.71V ~ 3.63V
Data Converters	A/D 28x12b; D/A 2x12b
Oscillator Type	Internal
Operating Temperature	-40°C ~ 85°C (TA)
Mounting Type	Surface Mount
Package / Case	100-TQFP
Supplier Device Package	100-TQFP (14x14)
Purchase URL	https://www.e-xfl.com/product-detail/microchip-technology/atsamd51n19a-aut

Email: info@E-XFL.COM

Address: Room A, 16/F, Full Win Commercial Centre, 573 Nathan Road, Mongkok, Hong Kong

**Processor and Architecture** 

Module	Source	Line
	MC 1	87
	MC 2	88
	MC 3	89
	MC 4	90
	MC 5	91
TCC1 - Timer Counter Control 1	CNT A	92
	DFS A	_
	ERR A	
	FAULTA A	_
	FAULTB A	
	FAULT0 A	_
	FAULT1 A	
	OVF	_
	TRG	
	UFS A	
	MC 0	93
	MC 1	94
	MC 2	95
	MC 3	96
TCC2 - Timer Counter Control 2	CNT A	97
	DFS A	_
	ERR A	
	FAULTA A	_
	FAULTB A	
	FAULT0 A	
	FAULT1 A	
	OVF	
	TRG	
	UFS A	
	MC 0	98
	MC 1	99
	MC 2	100

### **Processor and Architecture**

Module	Source	Line	
	RESRDY	119	
ADC1 - Analog Digital Converter 1	OVERRUN	120	
	WINMON		
	RESRDY	121	
AC - Analog Comparators	COMP 0	122	
	COMP 1		
	WIN 0		
DAC - Digital-to-Analog Converter	OVERRUN A 0	123	
	OVERRUN A 1		
	UNDERRUN A 0		
	UNDERRUN A 1		
	EMPTY 0	124	
	EMPTY 1	125	
	RESRDY 0	126	
	RESRDY 1	127	
I2S - Inter-IC Sound Interface	RXOR 0	128	
	RXOR 1		
	RXRDY 0		
	RXRDY 1		
	TXRDY 0		
	TXRDY 1		
	TXUR 0		
	TXUR 1		
PCC - Parallel Capture Controller	PCC	129	
AES - Advanced Encryption Standard	ENCCMP	130	
	GFMCMP		
TRNG - True Random Generator	ISO	131	
ICM - Integrity Check Monitor	ICM	132	
PUKCC - Public-Key Cryptography Controller	PUKCC	133	
QSPI - Quad SPI interface	QSPI	134	
SDHC0 - SD/MMC Host Controller 0	SDHC0	135	
	TIMER		

**GCLK - Generic Clock Controller** 



### 14.4 Signal Description Table 14-1. GCLK Signal Description

Signal Name	Туре	Description
GCLK_IO[7:0]	Digital I/O	Clock source for Generators when input
		Generic Clock signal when output

Note: One signal can be mapped on several pins.

#### **Related Links**

6. I/O Multiplexing and Considerations

#### 14.5 Product Dependencies

In order to use this peripheral, other parts of the system must be configured correctly, as described below.

#### 14.5.1 I/O Lines

Using the GCLK I/O lines requires the I/O pins to be configured.

#### **Related Links**

32. PORT - I/O Pin Controller

#### 14.5.2 Power Management

The GCLK can operate in sleep modes, if required. Refer to the sleep mode description in the Power Manager (PM) section.

#### **Related Links**

18. PM – Power Manager

### SUPC – Supply Controller

#### Name: BBPS Offset: 0x20 0x00000000 **Reset:** Property: **PAC Write-Protection** Bit 31 30 29 28 27 25 24 26 Access Reset Bit 23 22 21 20 19 18 17 16 Access Reset Bit 15 14 13 12 10 9 8 11 Access Reset 7 6 5 3 2 0 Bit 4 1 WAKEEN R/W Access Reset 0

### 19.8.9 Battery Backup Power Switch (BBPS) Control

#### Bit 2 – WAKEEN Wake Enable

Value	Description
0	The device is not woken up when switched from battery backup power to Main Power.
1	The device is woken up when switched from battery backup power to Main Power.

RTC – Real-Time Counter

Value	Description
0	There is not reset operation ongoing
1	The reset operation is ongoing

#### 22.8.5 CRC Status

Name:	CRCSTATUS
Offset:	0x0C
Reset:	0x00
Property:	PAC Write-Protection

Bit	7	6	5	4	3	2	1	0
						CRCERR	CRCZERO	CRCBUSY
Access						R	R	R/W
Reset						0	0	0

#### Bit 2 – CRCERR CRC Error

This bit is read '1' when the memory CRC monitor detects data corruption.

#### Bit 1 – CRCZERO CRC Zero

This bit is cleared when a new CRC source is selected.

This bit is set when the CRC generation is complete and the CRC Checksum is zero.

#### Bit 0 - CRCBUSY CRC Module Busy

When used with an I/O interface (CRCCTRL.CRCSRC=0x1):

- This bit is cleared by writing a '1' to it
- This bit is set when the CRC Data Input (CRCDATAIN) register is written
- Writing a '1' to this bit will clear the CRC Module Busy bit
- Writing a '0' to this bit has no effect

When used with a DMA channel (CRCCTRL.CRCSRC=0x20..,0x3F):

- This bit is cleared when the corresponding DMA channel is disabled
- This bit is set when the corresponding DMA channel is enabled
- Writing a '1' to this bit has no effect
- Writing a '0' to this bit has no effect

### **DMAC – Direct Memory Access Controller**

Value	Name	Description
0x5	6BEAT	6-beats burst length
0x6	7BEAT	7-beats burst length
0x7	8BEAT	8-beats burst length
0x8	9BEAT	9-beats burst length
0x9	10BEAT	10-beats burst length
0xA	11BEAT	11-beats burst length
0xB	12BEAT	12-beats burst length
0xC	13BEAT	13-beats burst length
0xD	14BEAT	14-beats burst length
0xE	15BEAT	15-beats burst length
0xF	16BEAT	16-beats burst length

#### Bits 21:20 – TRIGACT[1:0] Trigger Action

These bits define the trigger action used for a transfer. These bits are not enable-protected.

Value	Name	Description
0x0	BLOCK	One trigger required for each block transfer
0x1		Reserved
0x2	BURST	One trigger required for each burst transfer
0x3	TRANSACTION	One trigger required for each transaction

#### Bits 15:8 - TRIGSRC[7:0] Trigger Source

These bits define the peripheral that will be the source of a trigger.

Index	Instance	Channel	Presentation
0x00	DISABLE		Only software/event triggers
0x01	RTC	TIMESTAMP	DMA RTC timestamp trigger
0x02	DSU	DCC0	DMAC ID for DCC0 register
0x03	DSU	DCC1	DMAC ID for DCC1 register
0x04	SERCOM0	RX	Index of DMA RX trigger
0x05	SERCOM0	ТХ	Index of DMA TX trigger
0x06	SERCOM1	RX	Index of DMA RX trigger
0x07	SERCOM1	ТХ	Index of DMA TX trigger
0x08	SERCOM2	RX	Index of DMA RX trigger
0x09	SERCOM2	ТХ	Index of DMA TX trigger
0x0A	SERCOM3	RX	Index of DMA RX trigger
0x0B	SERCOM3	ТХ	Index of DMA TX trigger
0x0C	SERCOM4	RX	Index of DMA RX trigger
0x0D	SERCOM4	ТХ	Index of DMA TX trigger
0x0E	SERCOM5	RX	Index of DMA RX trigger

### **GMAC** - Ethernet MAC

Offset	Name	Bit Pos.						
		7:0	RX0[7:0]					
	15:8	RXO[15:8]						
0x0150	0x0150 ORLO	23:16	RXO[23:16]					
		31:24	RXO[31:24]					
		7:0	RXO[7:0]					
0x0154	OPHI	15:8	RXO[15:8]					
0X0154	OKHI	23:16						
		31:24						
		7:0	FRX[7:0]					
0v0158	FR	15:8	FRX[15:8]					
0.0130		23:16	FRX[23:16]					
		31:24	FRX[31:24]					
		7:0	BFRX[7:0]					
0x015C	BCER	15:8	BFRX[15:8]					
0,0100	Borte	23:16	BFRX[23:16]					
		31:24	BFRX[31:24]					
		7:0	MFRX[7:0]					
0x0160	MER	15:8	MFRX[15:8]					
0,0100		23:16	MFRX[23:16]					
		31:24	MFRX[31:24]					
		7:0	PFRX[7:0]					
0x0164	PFR	15:8	PFRX[15:8]					
		23:16						
		31:24						
		7:0	NFRX[7:0]					
0x0168	BFR64	15:8	NFRX[15:8]					
		23:16	NFRX[23:16]					
		31:24	NFRX[31:24]					
		7:0	NFRX[7:0]					
0x016C	TBFR127	15:8	NFRX[15:8]					
		23:16	NFRX[23:16]					
		31:24	NFRX[31:24]					
		7:0	NFRX[7:0]					
0x0170	TBFR255	15:8	NFRX[15:8]					
		23:16	NFRX[23:16]					
		31:24	NFRX[31:24]					
		7:0	NFRX[7:0]					
0x0174	TBFR511	15:8	NFRX[15:8]					
		23:16	NFRX[23:16]					
		31:24	NFRX[31:24]					
		7:0						
0x0178	TBFR1023	15:8						
		23:16	NFRX[23:10]					
		31:24	NFKX[31:24]					
0x017C	TBFR1518	/:0						
		15:8	NFRX[15:8]					

#### 24.9.21 GMAC Hash Register Top

Name:	HRT
Offset:	0x084
Reset:	0x00000000
Property:	Read/Write

The Unicast Hash Enable (UNIHEN) and the Multicast Hash Enable (MITIHEN) bits in the Network Configuration Register (NCFGR) enable the reception of hash matched frames.

Bit	31	30	29	28	27	26	25	24
Γ				ADDR	[31:24]			
Access	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W
Reset	0	0	0	0	0	0	0	0
Bit	23	22	21	20	19	18	17	16
Γ				ADDR	[23:16]			
Access	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W
Reset	0	0	0	0	0	0	0	0
Bit	15	14	13	12	11	10	9	8
Γ				ADDF	R[15:8]			
Access	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W
Reset	0	0	0	0	0	0	0	0
Bit	7	6	5	4	3	2	1	0
Γ				ADDI	R[7:0]			
Access	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W
Reset	0	0	0	0	0	0	0	0

Bits 31:0 - ADDR[31:0] Hash Address

Bits 63 to 32 of the Hash Address Register.

#### 24.9.39 GMAC Octets Transmitted High Register

Name:	OTHI
Offset:	0x104
Reset:	0x00000000
Property:	Read-Only

When reading the Octets Transmitted and Octets Received Registers, bits [31:0] should be read prior to bits [47:32] to ensure reliable operation.

Bit	31	30	29	28	27	26	25	24
Access								
Reset								
Bit	23	22	21	20	19	18	17	16
l								
Access								
Reset								
Bit	15	14	13	12	11	10	9	8
				ΤΧΟΙ	[15:8]			
Access	R	R	R	R	R	R	R	R
Reset	0	0	0	0	0	0	0	0
Bit	7	6	5	4	3	2	1	0
				TXO	[7:0]			
Access	R	R	R	R	R	R	R	R
Reset	0	0	0	0	0	0	0	0

#### Bits 15:0 - TXO[15:0] Transmitted Octets

Transmitted octets in valid frames of any type without errors, bits [47:32]. This counter is 48-bits, and is read through two registers. This count does not include octets from automatically generated pause frames.

#### 38.8.7 Host Registers - Pipe RAM

38.8.7.1 Pipe Descriptor Structure



#### 39.6.2.6 Bus Monitoring Mode

The CAN is set in Bus Monitoring Mode by programming CCCR.MON to '1'. In Bus Monitoring Mode (see ISO 11898-1, 10.12 Bus monitoring), the CAN is able to receive valid data frames and valid remote frames, but cannot start a transmission. In this mode, it sends only recessive bits on the CAN bus. If the CAN is required to send a dominant bit (ACK bit, overload flag, active error flag), the bit is rerouted internally so that the CAN monitors this dominant bit, although the CAN bus may remain in recessive state. In Bus Monitoring Mode register TXBRP is held in reset state.

The Bus Monitoring Mode can be used to analyze the traffic on a CAN bus without affecting it by the transmission of dominant bits. The figure below shows the connection of signals CAN\_TX and CAN\_RX to the CAN in Bus Monitoring Mode.

#### Figure 39-3. Pin Control in Bus Monitoring Mode



**Bus Monitoring Mode** 

#### 39.6.2.7 Disabled Automatic Retransmission

According to the CAN Specification (see ISO 11898-1, 6.3.3 Recovery Management), the CAN provides means for automatic retransmission of frames that have lost arbitration or that have been disturbed by errors during transmission. By default automatic retransmission is enabled. To support time-triggered communication as described in ISO 11898-1, chapter 9.2, the automatic retransmission may be disabled via CCCR.DAR.

Frame Transmission in DAR Mode

In DAR mode all transmissions are automatically cancelled after they started on the CAN bus. A Tx Buffer's Tx Request Pending bit TXBRP.TRPx is reset after successful transmission, when a transmission has not yet been started at the point of cancellation, has been aborted due to lost arbitration, or when an error occurred during frame transmission.

- Successful transmission:
  - Corresponding Tx Buffer Transmission Occurred bit TXBTO.TOx set
  - Corresponding Tx Buffer Cancellation Finished bit TXBCF.CFx not set
- Successful transmission in spite of cancellation:
  - Corresponding Tx Buffer Transmission Occurred bit TXBTO.TOx set
  - Corresponding Tx Buffer Cancellation Finished bit TXBCF.CFx set
- Arbitration lost or frame transmission disturbed:
  - Corresponding Tx Buffer Transmission Occurred bit TXBTO.TOx not set
  - Corresponding Tx Buffer Cancellation Finished bit TXBCF.CFx set

If HC2R.PVALEN = 1, this bit is automatically set to a value specified in one of the PVRx.

Value	Description
0	Divided Clock mode (BASECLK is used to generate SDCLK).
1	Programmable Clock mode (MULTCLK is used to generate SDCLK).

#### Bit 2 – SDCLKEN SD Clock Enable

The peripheral stops the SD Clock when writing this bit to 0. SDCLK Frequency Select (SDCLKFSEL) can be changed when this bit is 0. Then, the peripheral maintains the same clock frequency until SDCLK is stopped (Stop at SDCLK=0). If Card Inserted (CARDINS) in PSR is cleared, this bit is also cleared.

Value	Description
0	SD Clock disabled
1	SD Clock enabled

#### Bit 1 – INTCLKS Internal Clock Stable

This bit is set to 1 when the SD clock is stable after setting CCR.INTCLKEN (Internal Clock Enable) to 1. The user must wait to set SD Clock Enable (SDCLKEN) until this bit is set to 1.

Value	Description
0	Internal clock not ready
1	Internal clock ready

#### Bit 0 – INTCLKEN Internal Clock Enable

This bit is set to 0 when the peripheral is not used or is awaiting a wakeup interrupt. In this case, its internal clock is stopped to reach a very low power state. Registers are still able to be read and written. The clock starts to oscillate when this bit is set to 1. Once the clock oscillation is stable, the peripheral sets Internal Clock Stable (INTCLKS) in this register to 1.

This bit does not affect card detection.

Value	Description
0	The internal clock stops.
1	The internal clock oscillates.

### 42.4 Signal Description

Not applicable.

### 42.5 Product Dependencies

In order to use this AES module, other parts of the system must be configured correctly, as described below.

#### 42.5.1 I/O Lines

Not applicable.

#### 42.5.2 Power Management

The AES will continue to operate in Standby sleep mode, if it's source clock is running.

The AES interrupts can be used to wake up the device from Standby sleep mode. Refer to the Power Manager chapter for details on the different sleep modes.

AES is clocked only on the following conditions:

- When the DMA is enabled.
- Whenever there is an APB access for any read and write operation to the AES registers. (Not in Standby sleep mode.)
- When the AES is enabled & encryption/decryption is ongoing.

#### 42.5.3 Clocks

The AES bus clock (CLK\_AES\_APB) can be enabled and disabled in the Main Clock module, and the default state of CLK\_AES\_APB can be found in *Peripheral Clock Masking*. The module is fully clocked by CLK\_AES\_APB.

#### **Related Links**

15.6.2.6 Peripheral Clock Masking

#### 42.5.4 DMA

The AES has two DMA request lines; one for input data, and one for output data. They are both connected to the DMA Controller (DMAC). These DMA request triggers will be acknowledged by the DMAC ACK signals. Using the AES DMA requests requires the DMA Controller to be configured first. Refer to the device DMA documentation.

#### 42.5.5 Interrupts

The interrupt request line is connected to the interrupt controller. Using the AES interrupt requires the interrupt controller to be configured first. Refer to the Processor and Architecture chapter for details.

All the AES interrupts are synchronous wake-up sources. See Sleep Mode Controller for details.

#### **Related Links**

18.6.3.3 Sleep Mode Controller

#### 42.5.6 Events

Not applicable.

reduced value will be taken considering the high order words (potentially uninitialized) as part of the number, thus resulting in getting a mathematically correct but unexpected result.

In the case that the result is bigger than twice the modulus plus one word, the modular reduction feature has to be executed as a separate operation, using an Euclidean division.

#### 43.3.4.9.8 Constraints

The following conditions must be avoided to ensure that the service works correctly:

- nu1XBase, nu1YBase, nu1RBase or nu1ZBase are not aligned on 32-bit boundaries
- {nu1XBase, u2XLength}, {nu1YLength, u2YLength}, {nu1ZBase, u2XLength+u2YLength} or{nu1RBase, u2XLength+u2YLength} are not in Crypto RAM
- u2XLength, u2YLength is either: < 4, > 0xffc or not a 32-bit length
- {nu1RBase, u2XLength+u2YLength} overlaps {nu1YBase, u2YLength} or{nu1RBase, u2XLength +u2YLength} overlaps {nu1XBase, u2XLength}
- {nu1RBase, u2XLength+u2YLength} overlaps {nu1ZBase, u2XLength+u2YLength} and nu1RBase> nu1ZBase

If a modular reduction is specified, the relevant parameters must be defined according to the chosen reduction and follow the description in 43.3.5.1 Modular Reduction. Additional constraints to be respected and error codes are described in this section and in Table 43-49.

#### Multiplication with Accumulation or Subtraction

In the case where the options bits specify that either an Accumulation or a subtraction should be performed, this service performs the following operation:

 $R = (Z \pm (X \times Y + CarryOperand))mod B^{XLength + YLength}$ 

#### Table 43-27. Fmult Service (with Accumulate/Subtract From) Carry Settings

Option AND CARRYOPTIONS	CarryOperand	Resulting Operation
SET_CARRYOPTION(ADD_CARRY)	CarryIn	$R = Z \pm (X^*Y + CarryIn)$
SET_CARRYOPTION(SUB_CARRY)	- CarryIn	$R = Z \pm (X^*Y - CarryIn)$
SET_CARRYOPTION(ADD_1_PLUS_CARRY)	1 + CarryIn	$R = Z \pm (X^*Y + 1 + CarryIn)$
SET_CARRYOPTION(ADD_1_MINUS_CARRY)	1 - CarryIn	$R = Z \pm (X^*Y + 1 - CarryIn)$
SET_CARRYOPTION(CARRY_NONE)	0	$R = Z \pm (X^*Y)$
SET_CARRYOPTION(ADD_1)	1	$R = Z \pm (X^*Y + 1)$
SET_CARRYOPTION(SUB_1)	- 1	$R = Z \pm (X^*Y - 1)$
SET_CARRYOPTION(ADD_2)	2	$R = Z \pm (X^*Y + 2)$

#### Multiplication without Accumulation or Subtraction

In the case the options bits specify that either an Accumulation or a subtraction should be performed, this service performs the following operation:

 $R = (X \times Y + CarryOperand)mod B^{XLength + YLength}$ 

### Public Key Cryptography Controller (PUKCC)

Modular Reduction Form	Input Dynamic	Result Dynamic	Comments
	GF(2n): Input < ((P[x]) <sup>2</sup> ) * (X <sup>32</sup> )		
Normalized	InputLength < NLength + 4 bytes	GF(p): 0 ≤ Res < N GF(2 <sup>n</sup> ): Res < P[X]	The correction step does not runs in constant time. Needs a precomputed constant. The Normalize function cannot be applied to the product of two numbers of length u2NLength.
Using Euclidean division	InputLength < 2 * NLength + 4 bytes	GF(p): 0 ≤ Res < N GF(2 <sup>n</sup> ): Res < P[X]	Does not need any precomputed constant.

To be able to use these modular reduction services (except the Euclidean division), first the implementer shall call the setup service, providing the modulus as well as one free memory space for the constant (this constant is used to speed up the modular reduction). In most commands (except the modular exponentiation), the quotient is stored in the high order bytes of the number to be reduced, using only eight bytes more than the maximum size of the number to be reduced.

The following rules must be respected to ensure the modular reduction services function correctly:

- The numbers to be reduced can have any significant length, given the fact it CANNOT BE GREATER than 2\*u2ModLength + 4 bytes.
- The modulus SHALL ALWAYS HAVE a significant length of <u2ModLength> bytes. The modulus must be provided as a <u2ModLength + 4> bytes long number, padded on the most significant side with a 32-bit word cleared to zero. Not respecting this rule leads to unexpected and wrong results from the modular reduction.
- The normalization operation ALWAYS performs a modular reduction step, and will therefore have the same memory usage as this one.
- The very first operation before any modular operation SHALL BE a modular setup.

#### 43.3.5.1 Modular Reduction

#### 43.3.5.1.1 Purpose

This service is used to perform the various steps necessary to perform a modular reduction and accepts as input numbers in GF(p) or polynomials in  $GF(2^n)$ .

The available options for this service are:

- Work in the GF(2<sup>n</sup>) or in the standard integer arithmetic field GF(p)
- Operation is the generation of the reduction constant.
- Operation is a Modular Reduction.
- Operation is a Normalization.

#### 43.3.5.1.2 How to Use the Service

#### 43.3.5.1.3 Description

This service performs one of the following operations:

- {nu1ModBase, u2ModLength + 4}, {nu1CnsBase, u2ModLength + 8}, {nu1PointABase, 3\*u2ModLength + 12}, {nu1PointBBase, 3\*u2ModLength + 12}, {nu1Workspace, 
   WorkspaceLength>} are not in Crypto RAM
- u2ModLength is either: < 12, > 0xffc or not a 32-bit length
- All overlapping between {nu1ModBase, u2ModLength + 4}, {nu1CnsBase, u2ModLength +8}, {nu1PointABase, 3\*u2ModLength + 12}, {nu1PointBBase, 3\*u2ModLength + 12} and {nu1Workspace, 5\*u2ModLength + 32}

#### 43.3.6.3.7 Status Returned Values

#### Table 43-71. ZpEccAddFast Service Return Codes

Returned Status	Importance	Meaning
PUKCL_OK	-	The computation passed without problem.

#### 43.3.6.4 Fast Point Doubling

#### 43.3.6.4.1 Purpose

This service is used to perform a Point Doubling, based on a given elliptic curve over GF(p).

#### 43.3.6.4.2 How to Use the Service

#### 43.3.6.4.3 Description

These two services process the Point Doubling:

 $Pt_C = 2 \times Pt_A$ 

In this computation, the following parameters need to be provided:

- A the input point is filled in projective coordinates (X,Y,Z) (pointed by {nu1PointABase, 3\*u2ModLength + 12}). This point can be the Infinite Point.
- Cns the Fast Modular Constant filled (pointed by {nu1CnsBase,u2ModLength +8})
- P the modulus filled (pointed by {nu1ModBase,u2ModLength +4})
- The workspace not initialized (pointed by {nu1WorkSpace, 4\*u2ModLength +28}
- The a parameter relative to the elliptic curve (pointed by {nu1ABase,u2ModLength +4})
- The resulting C point is represented in projective coordinates (X,Y,Z) and is stored at the same location than the input point A. This point can be the Infinite Point.

The service name for this operation is <code>ZpEccDblFast</code>. This service uses Fast mode and Fast Modular Reduction for computations.



**Important:** Before using this service, ensure that the constant Cns has been calculated with the setup of the Fast Modular Reduction service.

#### **TCC – Timer/Counter for Control Applications**

Pin Name	Туре	Description
TCC/WO[WO_NUM-1]	Digital output	Compare channel n waveform output

Refer to *I/O Multiplexing and Considerations* for details on the pin mapping for this peripheral. One signal can be mapped on several pins.

#### **Related Links**

6. I/O Multiplexing and Considerations

#### 49.5 **Product Dependencies**

In order to use this peripheral, other parts of the system must be configured correctly, as described below.

#### 49.5.1 I/O Lines

In order to use the I/O lines of this peripheral, the I/O pins must be configured using the I/O Pin Controller (PORT).

#### **Related Links**

32. PORT - I/O Pin Controller

#### 49.5.2 Power Management

This peripheral can continue to operate in any sleep mode where its source clock is running. The interrupts can wake up the device from sleep modes. Events connected to the event system can trigger other operations in the system without exiting sleep modes.

#### 49.5.3 Clocks

The TCC bus clocks (CLK\_TCCx\_APB) can be enabled and disabled in the Main Clock module. The default state of CLK\_TCCx\_APB can be found in the Peripheral Clock Masking section (see the Related Links below).

A generic clock (GCLK\_TCCx) is required to clock the TCC. This clock must be configured and enabled in the generic clock controller before using the TCC.

The generic clocks (GCLK\_TCCx) are asynchronous to the bus clock (CLK\_TCCx\_APB). Due to this asynchronicity, writing certain registers will require synchronization between the clock domains. Refer to 49.6.7 Synchronization for further details.

#### **Related Links**

15.6.2.6 Peripheral Clock Masking14. GCLK - Generic Clock Controller

#### 49.5.4 DMA

The DMA request lines are connected to the DMA Controller (DMAC). In order to use DMA requests with this peripheral the DMAC must be configured first. Refer to *DMAC – Direct Memory Access Controller* for details.

#### **Related Links**

22. DMAC – Direct Memory Access Controller

© 2018 Microchip Technology Inc.

**I2S - Inter-IC Sound Controller** 

Offset	Name	Bit Pos.	
		15:8	DATA[15:8]
		23:16	DATA[23:16]
		31:24	DATA[31:24]
0x34	RXDATA	7:0	DATA[7:0]
		15:8	DATA[15:8]
		23:16	DATA[23:16]
		31:24	DATA[31:24]

#### 51.9 Register Description

Registers can be 8, 16, or 32 bits wide. Atomic 8-, 16-, and 32-bit accesses are supported. In addition, the 8-bit quarters and 16-bit halves of a 32-bit register, and the 8-bit halves of a 16-bit register can be accessed directly.

Some registers require synchronization when read and/or written. Synchronization is denoted by the "Read-Synchronized" and/or "Write-Synchronized" property in each individual register description.

Some registers are enable-protected, meaning they can only be written when the module is disabled. Enable-protection is denoted by the "Enable-Protected" property in each individual register description.

Optional write-protection by the Peripheral Access Controller (PAC) is denoted by the "PAC Write-Protection" property in each individual register description.

### Electrical Characteristics at 85°C

Sleep Mode	Conditions	Тур	Unit
	STDBYCFG.FASTWKUP = 2 Fast Wakeup is enabled on the main voltage regulator.	25	μs
	STDBYCFG.FASTWKUP = 3 Fast Wakeup is enabled on both NVM and MAINVREG.	5	μs
Hibernate		320	μs
BACKUP		350	μs
OFF		210	μs

#### 54.9 I/O Pin Characteristics

The pins have two different speeds controlled by the Drive Strength bit located in the Pin Configuration register PORT (PORT.PINCFG.DRVSTR).

#### Table 54-14. I/O Pins Common Characteristics

Symbol	Parameter	Conditions	Min.	Тур.	Max.	Units
V <sub>IL</sub>	Input Low-Level Voltage	V <sub>DD</sub> = 1.71V-3.6V	-	-	$0.3 \times V_{DD}$	V
V <sub>IH</sub>	Input High-Level Voltage	V <sub>DD</sub> = 1.71V-3.6V	$0.7 \times V_{DD}$	-	-	
V <sub>OL</sub>	Output Low-Level Voltage	V <sub>DD</sub> > 1.71V, I <sub>OL</sub> max	-	$0.1 \times V_{DD}$	$0.2 \times V_{DD}$	
V <sub>OH</sub>	Output High-Level Voltage	V <sub>DD</sub> > 1.71V, I <sub>OH</sub> max	$0.8 \times V_{DD}$	$0.9 \times V_{DD}$	-	
R <sub>PULL</sub>	Pull-up - Pull-down Resistance	-	20	40	60	kΩ
	Pull-down resistance on pads PA24 and PA25	-	14	23	28	
I <sub>LEAK</sub>	Input Leakage Current	Pull-up resistors disabled	-1	±0.015	1	μA

#### Table 54-15. I/O Pins Maximum Output Current<sup>(2,3)</sup>

Symbol	Parameter	Conditions	Backup Pins in Backup Mode	Backup and Normal Pins	Backup and Normal Pins	Units
				DRVSTR=0	DRVSTR=1	
I <sub>OL</sub>	Maximum Output low- level current	V <sub>DD</sub> =1.71V-3V	0.005	0.5	3	mA
		V <sub>DD</sub> =3V-3.63V	0.01	2	8	
I <sub>OH</sub>	Maximum Output high-	V <sub>DD</sub> =1.71V-3V	0.005	0.5	3	
	level current	V <sub>DD</sub> =3V-3.63V	0.01	2	8	