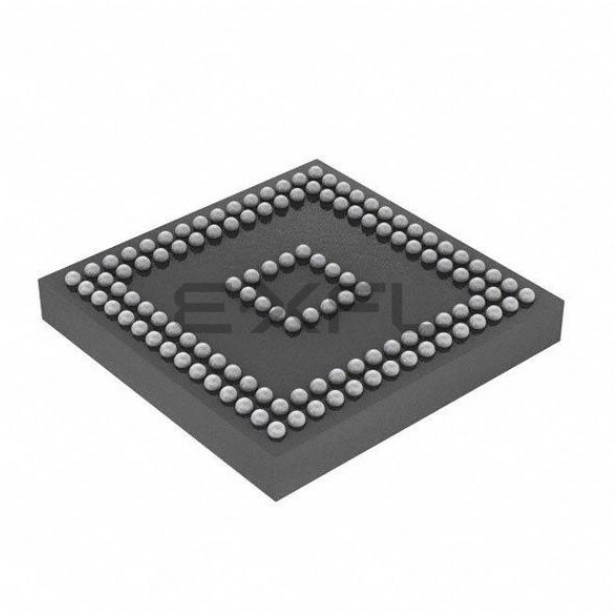


Welcome to E-XFL.COM

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 "Embedded - Microcontrollers"

Details	
Product Status	Active
Core Processor	ARM® Cortex®-M4F
Core Size	32-Bit Single-Core
Speed	120MHz
Connectivity	CANbus, EBI/EMI, Ethernet, I²C, IrDA, LINbus, MMC/SD, QSPI, SPI, UART/USART, USB
Peripherals	Brown-out Detect/Reset, DMA, I²S, POR, PWM, WDT
Number of I/O	99
Program Memory Size	1MB (1M x 8)
Program Memory Type	FLASH
EEPROM Size	-
RAM Size	256K x 8
Voltage - Supply (Vcc/Vdd)	1.71V ~ 3.63V
Data Converters	A/D 32x12b; D/A 2x12b
Oscillator Type	Internal
Operating Temperature	-40°C ~ 85°C (TA)
Mounting Type	Surface Mount
Package / Case	120-TFBGA
Supplier Device Package	120-TFBGA (8x8)
Purchase URL	https://www.e-xfl.com/product-detail/microchip-technology/atsame54p20a-ctut

Value	Description
0	The APBB clock for the SERCOMn is stopped.
1	The APBB clock for the SERCOMn is enabled.

Bit 7 – EVSYS EVSYS APBB Clock Enable

Value	Description
0	The APBB clock for the EVSYS is stopped.
1	The APBB clock for the EVSYS is enabled.

Bit 4 – PORT PORT APBB Clock Enable

Value	Description
0	The APBB clock for the PORT is stopped.
1	The APBB clock for the PORT is enabled.

Bit 2 – NVMCTRL NVMCTRL APBB Clock Enable

Value	Description
0	The APBB clock for the NVMCTRL is stopped.
1	The APBB clock for the NVMCTRL is enabled.

Bit 1 – DSU DSU APBB Clock Enable

Value	Description
0	The APBB clock for the DSU is stopped.
1	The APBB clock for the DSU is enabled.

Bit 0 – USB USB APBB Clock Enable

Value	Description
0	The APBB clock for the USB is stopped.
1	The APBB clock for the USB is enabled.

20.6.7 Synchronization

Due to asynchronicity between the main clock domain and the peripheral clock domains, some registers need to be synchronized when written or read.

The following registers are synchronized when written:

- Enable bit in Control A register (CTRLA.ENABLE)
- Window Enable bit in Control A register (CTRLA.WEN)
- Always-On bit in control Control A (CTRLA.ALWAYSON)
- Watchdog Clear register (CLEAR)

Required write-synchronization is denoted by the "Write-Synchronized" property in the register description.

Required read-synchronization is denoted by the "Read-Synchronized" property in the register description.

20.6.8 Additional Features

20.6.8.1 Always-On Mode

The Always-On mode is enabled by setting the Always-On bit in the Control A register (CTRLA.ALWAYSON=1). When the Always-On mode is enabled, the WDT runs continuously, regardless of the state of CTRLA.ENABLE. Once written, the Always-On bit can only be cleared by a power-on reset. The Configuration (CONFIG) and Early Warning Control (EWCTRL) registers are read-only registers while the CTRLA.ALWAYSON bit is set. Thus, the time period configuration bits (CONFIG.PER, CONFIG.WINDOW, EWCTRL.EWOFFSET) of the WDT cannot be changed.

Enabling or disabling Window mode operation by writing the Window Enable bit (CTRLA.WEN) is allowed while in Always-On mode, but note that CONFIG.PER cannot be changed.

The Interrupt Clear and Interrupt Set registers are accessible in the Always-On mode. The Early Warning interrupt can still be enabled or disabled while in the Always-On mode, but note that EWCTRL.EWOFFSET cannot be changed.

Table WDT Operating Modes With Always-On shows the operation of the WDT for CTRLA.ALWAYSON=1.

Table 20-2. WDT Operating Modes With Always-On

WEN	Interrupt Enable	Mode
0	0	Always-on and normal mode
0	1	Always-on and normal mode with Early Warning interrupt
1	0	Always-on and window mode
1	1	Always-on and window mode with Early Warning interrupt

20.6.8.2 Early Warning

The Early Warning interrupt notifies that the WDT is approaching its time-out condition. The Early Warning interrupt behaves differently in Normal mode and in Window mode.

In Normal mode, the Early Warning interrupt generation is defined by the Early Warning Offset in the Early Warning Control register (EWCTRL.EWOFFSET). The Early Warning Offset bits define the number of CLK_WDT_OSC clocks before the interrupt is generated, relative to the start of the watchdog time-out period.

21.8.15 Tamper ID

Name: TAMPID
Offset: 0x68
Reset: 0x00000000

Bit	31	30	29	28	27	26	25	24
	TAMPEVT							
Access	R/W							
Reset	0							

Bit	23	22	21	20	19	18	17	16
Access								
Reset								

Bit	15	14	13	12	11	10	9	8
Access								
Reset								

Bit	7	6	5	4	3	2	1	0
				TAMPID4	TAMPID3	TAMPID2	TAMPID1	TAMPID0
Access				R/W	R/W	R/W	R/W	R/W
Reset				0	0	0	0	0

Bit 31 – TAMPEVT Tamper Event Detected
Writing a '0' to this bit has no effect. Writing a '1' to this bit clears the tamper detection bit.

Value	Description
0	A tamper input event has not been detected
1	A tamper input event has been detected

Bits 0, 1, 2, 3, 4 – TAMPID Tamper on Channel n Detected
Writing a '0' to this bit has no effect. Writing a '1' to this bit clears the tamper detection bit.

Value	Description
0	A tamper condition has not been detected on Channel n
1	A tamper condition has been detected on Channel n

21.10.10 Counter Value in COUNT16 mode (CTRLA.MODE=1)

Name: COUNT
Offset: 0x18
Reset: 0x0000
Property: PAC Write-Protection, Write-Synchronized, Read-Synchronized

Bit	15	14	13	12	11	10	9	8
	COUNT[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
	COUNT[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 15:0 – COUNT[15:0] Counter Value
These bits define the value of the 16-bit RTC counter in COUNT16 mode (CTRLA.MODE=1).

21.12.1 Control A in Clock/Calendar mode (CTRLA.MODE=2)

Name: CTRLA
Offset: 0x00
Reset: 0x0000
Property: PAC Write-Protection, Enable-Protected, Write-Synchronized

Bit	15	14	13	12	11	10	9	8
	CLOCKSYNC	GPTRST			PRESCALER[3:0]			
Access	R/W	R/W			R/W	R/W	R/W	R/W
Reset	0	0			0	0	0	0

Bit	7	6	5	4	3	2	1	0
	MATCHCLR	CLKREP			MODE[1:0]		ENABLE	SWRST
Access	R/W	R/W			R/W	R/W	R/W	R/W
Reset	0	0			0	0	0	0

Bit 15 – CLOCKSYNC CLOCK Read Synchronization Enable
The CLOCK register requires synchronization when reading. Disabling the synchronization will prevent reading valid values from the CLOCK register.
This bit is not enable-protected.

Value	Description
0	CLOCK read synchronization is disabled
1	CLOCK read synchronization is enabled

Bit 14 – GPTRST GP Registers Reset On Tamper Enable
Only GP registers enabled by the CTRLB.GPnEN bits are affected. This bit can be written only when the peripheral is disabled.
This bit is not synchronized.

Bits 11:8 – PRESCALER[3:0] Prescaler
These bits define the prescaling factor for the RTC clock source (GCLK_RTC) to generate the counter clock (CLK_RTC_CNT). Periodic events and interrupts are not available when the prescaler is off. These bits are not synchronized.

Value	Name	Description
0x0	OFF	CLK_RTC_CNT = GCLK_RTC/1
0x1	DIV1	CLK_RTC_CNT = GCLK_RTC/1
0x2	DIV2	CLK_RTC_CNT = GCLK_RTC/2
0x3	DIV4	CLK_RTC_CNT = GCLK_RTC/4
0x4	DIV8	CLK_RTC_CNT = GCLK_RTC/8
0x5	DIV16	CLK_RTC_CNT = GCLK_RTC/16
0x6	DIV32	CLK_RTC_CNT = GCLK_RTC/32
0x7	DIV64	CLK_RTC_CNT = GCLK_RTC/64
0x8	DIV128	CLK_RTC_CNT = GCLK_RTC/128
0x9	DIV256	CLK_RTC_CNT = GCLK_RTC/256
0xA	DIV512	CLK_RTC_CNT = GCLK_RTC/512

22.10.4 Block Transfer Destination Address

Name: DSTADDR
Offset: 0x08
Property: -

The DSTADDR register offset is relative to (BASEADDR or WRBADDR) + Channel Number * 0x10

Bit	31	30	29	28	27	26	25	24
	DSTADDR[31:24]							
Access								
Reset								

Bit	23	22	21	20	19	18	17	16
	DSTADDR[23:16]							
Access								
Reset								

Bit	15	14	13	12	11	10	9	8
	DSTADDR[15:8]							
Access								
Reset								

Bit	7	6	5	4	3	2	1	0
	DSTADDR[7:0]							
Access								
Reset								

Bits 31:0 – DSTADDR[31:0] Transfer Destination Address
This bit group holds the destination address corresponding to the last beat transfer address in the block transfer.

Bit 15 – SRTSM Store Receive Time Stamp to Memory
Writing a '1' to this bit causes the CRC of every received frame to be replaced with the value of the nanoseconds field of the 1588 timer that was captured as the receive frame passed the message time stamp point.

Value	Description
0	Normal operation
1	All received frames' CRC is replaced with a time stamp

Bit 12 – TXZQPF Transmit Zero Quantum Pause Frame
Writing a '1' to this bit causes a pause frame with zero quantum to be transmitted.

Writing a '0' to this bit has no effect.

Bit 11 – TXPF Transmit Pause Frame
Writing one to this bit causes a pause frame to be transmitted.

Writing a '0' to this bit has no effect.

Bit 10 – THALT Transmit Halt
Writing a '1' to this bit halts transmission as soon as any ongoing frame transmission ends.

Writing a '0' to this bit has no effect.

Bit 9 – TSTART Start Transmission
Writing a '1' to this bit starts transmission.

Writing a '0' to this bit has no effect.

Bit 8 – BP Back Pressure
In 10M or 100M half duplex mode, writing a '1' to this bit forces collisions on all received frames. Ignored in gigabit half duplex mode.

Value	Description
0	Frame collisions are not forced
1	Frame collisions are forced in 10M and 100M half duplex mode

Bit 7 – WESTAT Write Enable for Statistics Registers
Writing a '1' to this bit makes the statistics registers writable for functional test purposes.

Value	Description
0	Statistics Registers are write-protected
1	Statistics Registers are write-enabled

Bit 6 – INCSTAT Increment Statistics Registers
Writing a '1' to this bit increments all Statistics Registers by one for test purposes.

Writing a '0' to this bit has no effect.

This bit will always read '0'.

Bit 5 – CLRSTAT Clear Statistics Registers
Writing a '1' to this bit clears the Statistics Registers.

Writing a '0' to this bit has no effect.

Related Links

26.6.3 Region Descriptor Structure

Value	Description
0	Peripheral is not write protected
1	Peripheral is write protected

Bit 11 – ICM ICM APB Protection Enable

Value	Description
0	Peripheral is not write protected
1	Peripheral is write protected

Bit 10 – TRNG TRNG APB Protection Enable

Value	Description
0	Peripheral is not write protected
1	Peripheral is write protected

Bit 9 – AES AES APB Protection Enable

Value	Description
0	Peripheral is not write protected
1	Peripheral is write protected

Bit 8 – AC AC APB Protection Enable

Value	Description
0	Peripheral is not write protected
1	Peripheral is write protected

Bit 7 – PDEC PDEC APB Protection Enable

Value	Description
0	Peripheral is not write protected
1	Peripheral is write protected

Bit 6 – TC5 TC5 APB Protection Enable

Value	Description
0	Peripheral is not write protected
1	Peripheral is write protected

Bit 5 – TC4 TC4 APB Protection Enable

Value	Description
0	Peripheral is not write protected
1	Peripheral is write protected

Bit 4 – TCC3 TCC3 APB Protection Enable

Value	Description
0	Peripheral is not write protected
1	Peripheral is write protected

Value	Description
0	DAC is not write protected
1	DAC is write protected

Bit 8 – ADC1 ADC1 APB Protect Enable

Value	Description
0	ADC1 is not write protected
1	ADC1 is write protected

Bit 7 – ADC0 ADC0 APB Protect Enable

Value	Description
0	ADC0 is not write protected
1	ADC0 is write protected

Bit 6 – TC7 TC7 APB Protect Enable

Value	Description
0	TC7 is not write protected
1	TC7 is write protected

Bit 5 – TC6 TC6 APB Protect Enable

Value	Description
0	TC6 is not write protected
1	TC6 is write protected

Bit 4 – TCC4 TCC4 APB Protect Enable

Value	Description
0	TCC4 is not write protected
1	TCC4 is write protected

Bit 3 – SERCOM7 SERCOM7 APB Protect Enable

Value	Description
0	SERCOM7 is not write protected
1	SERCOM7 is write protected

Bit 2 – SERCOM6 SERCOM6 APB Protect Enable

Value	Description
0	SERCOM6 is not write protected
1	SERCOM6 is write protected

Bit 1 – SERCOM5 SERCOM5 APB Protect Enable

Value	Description
0	SERCOM5 is not write protected
1	SERCOM5 is write protected

Writing a zero to this bit has no effect.

Writing a '1' to this bit clears the DPLL1 Lock Fall interrupt flag.

Bit 24 – DPLL1LCKR DPLL1 Lock Rise
This flag is cleared by writing a '1' to it.

This flag is set on a zero-to-one transition of the DPLL1 Lock Rise bit in the Status register (STATUS.DPLL1LCKR) and will generate an interrupt request if INTENSET.DPLL1LCKR is '1'.

Writing a zero to this bit has no effect.

Writing a '1' to this bit clears the DPLL1 Lock Rise interrupt flag.

Bit 19 – DPLL0LDRTO DPLL0 Loop Divider Ratio Update Complete
This flag is cleared by writing a '1' to it.

This flag is set on a zero-to-one transition of the DPLL0 Loop Divider Ratio Update Complete bit in the Status register (STATUS.DPLL0LDRTO) and will generate an interrupt request if INTENSET.DPLL0LDRTO is '1'.

Writing a zero to this bit has no effect.

Writing a '1' to this bit clears the DPLL0 Loop Divider Ratio Update Complete interrupt flag.

Bit 18 – DPLL0LTO DPLL0 Lock Timeout
This flag is cleared by writing a '1' to it.

This flag is set on a zero-to-one transition of the DPLL0 Lock Timeout bit in the Status register (STATUS.DPLL0LTO) and will generate an interrupt request if INTENSET.DPLL0LTO is '1'.

Writing a zero to this bit has no effect.

Writing a '1' to this bit clears the DPLL0 Lock Timeout interrupt flag.

Bit 17 – DPLL0LCKF DPLL0 Lock Fall
This flag is cleared by writing a '1' to it.

This flag is set on a zero-to-one transition of the DPLL0 Lock Fall bit in the Status register (STATUS.DPLL0LCKF) and will generate an interrupt request if INTENSET.DPLL0LCKF is '1'.

Writing a zero to this bit has no effect.

Writing a '1' to this bit clears the DPLL0 Lock Fall interrupt flag.

Bit 16 – DPLL0LCKR DPLL0 Lock Rise
This flag is cleared by writing a '1' to it.

This flag is set on a zero-to-one transition of the DPLL0 Lock Rise bit in the Status register (STATUS.DPLL0LCKR) and will generate an interrupt request if INTENSET.DPLL0LCKR is '1'.

Writing a zero to this bit has no effect.

Writing a '1' to this bit clears the DPLL0 Lock Rise interrupt flag.

Bit 12 – DFLLRCS DFLL Reference Clock Stopped
This flag is cleared by writing a '1' to it.

29. OSC32KCTRL – 32KHz Oscillators Controller

29.1 Overview

The 32KHz Oscillators Controller (OSC32KCTRL) provides a user interface to the 32.768kHz oscillators: XOSC32K and OSCULP32K.

The OSC32KCTRL sub-peripherals can be enabled, disabled, calibrated, and monitored through interface registers.

All sub-peripheral statuses are collected in the Status register (STATUS). They can additionally trigger interrupts upon status changes through the INTENSET, INTENCLR, and INTFLAG registers.

29.2 Features

- 32.768kHz Crystal Oscillator (XOSC32K)
  - Programmable start-up time
  - Crystal or external input clock on XIN32 I/O
  - Clock failure detection with safe clock switch
  - Clock failure event output
- 32.768kHz Ultra Low-Power Internal Oscillator (OSCULP32K)
  - Ultra low-power, always-on oscillator
  - Frequency fine tuning
- Calibration value loaded from Flash factory calibration at Reset
- 1.024 kHz clock outputs available

29.8.2 Interrupt Enable Set

Name: INTENSET
Offset: 0x04
Reset: 0x00000000
Property: PAC Write-Protection

This register allows the user to disable an interrupt without doing a read-modify-write operation. Changes in this register will also be reflected in the Interrupt Enable Clear register (INTENCLR).

Bit	31	30	29	28	27	26	25	24
Access								
Reset								

Bit	23	22	21	20	19	18	17	16
Access								
Reset								

Bit	15	14	13	12	11	10	9	8
Access								
Reset								

Bit	7	6	5	4	3	2	1	0
						XOSC32KFAIL		XOSC32KRDY
Access						R/W		R/W
Reset						0		0

Bit 2 – XOSC32KFAIL XOSC32K Clock Failure Detector Interrupt Enable
Writing a '0' to this bit has no effect.

Writing a '1' to this bit will set the XOSC32K Clock Failure Interrupt Enable bit, which enables the XOSC32K Clock Failure interrupt.

Value	Description
0	The XOSC32K Clock Failure Detection is disabled.
1	The XOSC32K Clock Failure Detection is enabled. An interrupt request will be generated when the XOSC32K Clock Failure Detection interrupt flag is set.

Bit 0 – XOSC32KRDY XOSC32K Ready Interrupt Enable
Writing a '0' to this bit has no effect.

Writing a '1' to this bit will set the XOSC32K Ready Interrupt Enable bit, which enables the XOSC32K Ready interrupt.

Value	Description
0	The XOSC32K Ready interrupt is disabled.
1	The XOSC32K Ready interrupt is enabled.

39.8.21 Standard ID Filter Configuration

Name: SIDFC
Offset: 0x84
Reset: 0x00000000
Property: Write-restricted

This register is write-restricted and only writable if bit fields CCCR.CCE = 1 and CCCR.INIT = 1.

Bit	31	30	29	28	27	26	25	24
Access								
Reset								

Bit	23	22	21	20	19	18	17	16
	LSS[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

Bit	15	14	13	12	11	10	9	8
	FLSSA[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
	FLSSA[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 23:16 – LSS[7:0] List Size Standard

Value	Description
0	No standard Message ID filter.
1 - 128	Number of standard Message ID filter elements.
> 128	Values greater than 128 are interpreted as 128.

Bits 15:0 – FLSSA[15:0] Filter List Standard Start Address
Start address of standard Message ID filter list. When the CAN module addresses the Message RAM it addresses 32-bit words, not single bytes. The configurable start addresses are 32-bit word addresses, i.e. only bits 15 to 2 are evaluated, the two least significant bits are ignored. Bits 1 to 0 will always be read back as “00”.

Table 39-15. Extended Message ID Filter Element

	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
F0	EFEC[2:0]			EFID1[28:0]																												
F1	EFT[1:0]			EFID2[28:0]																												

- F0 Bits 31:29 - EFEC[2:0]: Extended Filter Element Configuration

  All enabled filter elements are used for acceptance filtering of extended frames. Acceptance filtering stops at the first matching enabled filter element or when the end of the filter list is reached. If EFEC = “100”, “101”, or “110” a match sets interrupt flag IR.HPM and, if enabled, an interrupt is generated. In this case register HPMS is updated with the status of the priority match.

Table 39-16. Extended Filter Element Configuration

Value	Name	Description
0x0	DISABLE	Disable filter element.
0x1	STF0M	Store in Rx FIFO 0 if filter matches.
0x2	STF1M	Store in Rx FIFO 1 if filter matches.
0x3	REJECT	Reject ID if filter matches.
0x4	PRIORITY	Set priority if filter matches.
0x5	PRIF0M	Set priority and store in FIFO 0 if filter matches.
0x6	PRIF1M	Set priority and store in FIFO 1 if filter matches.
0x7	STRXBUF	Store into Rx Buffer or as debug message, configuration of EFT[1:0] ignored.

- F0 Bits 28:0 - EFID1[28:0]: Extended Filter ID 1

  First ID of extended ID filter element.

  When filtering for Rx Buffers or for debug messages this field defines the ID of a extended mesage to be stored. The received identifiers must match exactly, only XIDAM masking mechanism is used.
- F1 Bits 31:30 - EFT[1:0]: Extended Filter Type

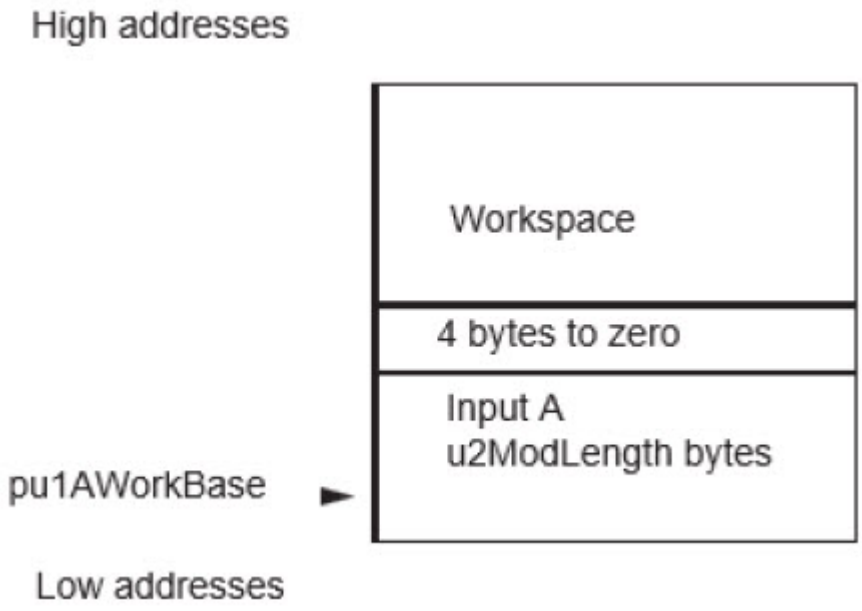
  This field defines the extended filter type.

Table 39-17. Extended Filter Type

Value	Name	Description
0x0	RANGEM	Range filter from EFID1 to EFID2 (EFID2 >= EFID1).
0x1	DUAL	Dual ID filter for EFID1 or EFID2.
0x2	CLASSIC	Classic filter: EFID1 = filter, EFID2 = mask.
0x3	RANGE	Range filter from EFID1 to EFID2 (EFID2 >= EFID1), XIDAM mask not applied.

- F1 Bits 28:0 - EFID2[28:0]: Extended Filter ID 2

Figure 43-14. The a parameter and Workspace {pu1AWorkBase, 9*u2ModLength + 48}



43.3.7 Elliptic Curves Over GF(2^n) Services

This section provides a complete description of the currently available elliptic curve over Polynomials in GF(2^n) services.

These services process Polynomials in GF(2^n) only.

The offered services cover the basic operations over elliptic curves such as:

- Adding two points over a curve
- Doubling a point over a curve
- Multiplying a point by an integral constant
- Converting a point's projective coordinates (resulting from a doubling or an addition) to the affine coordinates, and oppositely converting a point's affine coordinates to the projective coordinates.
- Testing the point presence on the curve.

Additionally, some higher level services covering the needs for signature generation and verification are offered:

- Generating an ECDSA signature (compliant with FIPS186-2)
- Verifying an ECDSA signature (compliant with FIPS 186-2) The supported curves use the following curve equation in GF(2^n):

$Y^2 + XY = X^3 + aX + b$

43.3.7.1 Parameters Format

43.3.7.1.1 Polynomials in GF(2^n)

Polynomials in GF(2^n) are binary polynomials reduced modulo the polynomial P[X]. This polynomial is called the modulus and may be abbreviated to P in this document. The storage of these polynomials in memory area is described in 43.3.3.4 Aligned Significant Length.

For notation simplicity the comparison signs "<" or ">" may be used for polynomials, this is to be interpreted as a comparison between the degree of the polynomials.

43.3.7.3.2 How to Use the Service

43.3.7.3.3 Description

The operation performed is:

$Pt_C = 2 \times Pt_A$

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 and b Parameters relative to the Elliptic Curve Equation (pointed by {nu1ABBase, 2*u2ModLength+ 8})
- The resulting C point is represented in projective coordinates (X,Y,Z) and is stored at the very same place than the input point A. This point can be the Infinite Point.

The service name for this operation is `GF2NEccDblFast`. This service uses Fast mode and Fast Modular Reduction for computation.

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

43.3.7.3.4 Parameters Definition

Table 43-96. GF2NEccDblFast Service Parameters

Parameter	Type	Direction	Location	Data Length	Before Executing the Service	After Executing the Service
nu1ModBase	nu1	I	Crypto RAM	u2ModLength + 4	Base of modulus P	Base of modulus P
nu1CnsBase	nu1	I	Crypto RAM	u2ModLength + 12	Base of Cns	Base of Cns
u2ModLength	u2	I	–	–	Length of modulus P	Length of modulus P
nu1ABBase	u2	I	Crypto RAM	2*u2ModLength + 8	Parameters a and b of the elliptic curve	Parameter a and b of the elliptic curve
nu1PointABase	nu1	I/O	Crypto RAM	3*u2ModLength + 12	Input point A (projective coordinates)	Resulting point C (projective coordinates)
nu1Workspace	nu1	I	Crypto RAM	4*u2ModLength + 28	–	Corrupted workspace

46.7 Register Summary

Offset	Name	Bit Pos.								
0x00	CTRLA	7:0							ENABLE	SWRST
0x01	CTRLB	7:0							STARTx	STARTx
0x02	EVCTRL	7:0				WINEO0			COMPEOx	COMPEOx
		15:8			INVEIx	INVEIx			COMPEIx	COMPEIx
0x04	INTENCLR	7:0				WIN0			COMPx	COMPx
0x05	INTENSET	7:0				WIN0			COMPx	COMPx
0x06	INTFLAG	7:0				WIN0			COMPx	COMPx
0x07	STATUSA	7:0			WSTATE0[1:0]				STATEx	STATEx
0x08	STATUSB	7:0							READYx	READYx
0x09	DBGCTRL	7:0								DBGRUN
0x0A	WINCTRL	7:0						WINTSEL0[1:0]		WEN0
0x0B	Reserved									
0x0C	SCALER0	7:0			VALUE[5:0]					
0x0D	SCALER1	7:0			VALUE[5:0]					
0x0E ... 0x0F	Reserved									
0x10	COMPCTRL0	7:0		RUNSTDBY		INTSEL[1:0]		SINGLE	ENABLE	
		15:8	SWAP	MUXPOS[2:0]				MUXNEG[2:0]		
		23:16			HYST[1:0]		HYSTEN		SPEED[1:0]	
		31:24			OUT[1:0]			FLEN[2:0]		
0x14	COMPCTRL1	7:0		RUNSTDBY		INTSEL[1:0]		SINGLE	ENABLE	
		15:8	SWAP	MUXPOS[2:0]				MUXNEG[2:0]		
		23:16			HYST[1:0]		HYSTEN		SPEED[1:0]	
		31:24			OUT[1:0]			FLEN[2:0]		
0x18 ... 0x1F	Reserved									
0x20	SYNCBUSY	7:0				COMPCTRLx	COMPCTRLx	WINCTRL	ENABLE	SWRST
		15:8								
		23:16								
		31:24								
0x24	CALIB	7:0							BIAS0[1:0]	
		15:8								

46.8 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 are optionally write-protected by the Peripheral Access Controller (PAC). Optional PAC write-protection is denoted by the "PAC Write-Protection" property in each individual register description. For details, refer to Register Access Protection.

46.8.5 Interrupt Enable Set

Name: INTENSET
Offset: 0x05
Reset: 0x00
Property: PAC Write-Protection

This register allows the user to enable an interrupt without doing a read-modify-write operation. Changes in this register will also be reflected in the Interrupt Enable Clear register (INTENCLR).

Bit	7	6	5	4	3	2	1	0
				WIN0			COMPx	COMPx
Access				R/W			R/W	R/W
Reset				0			0	0

Bit 4 – WIN0 Window 0 Interrupt Enable
Reading this bit returns the state of the Window 0 interrupt enable.

Writing a '0' to this bit has no effect.

Writing a '1' to this bit enables the Window 0 interrupt.

Value	Description
0	The Window 0 interrupt is disabled.
1	The Window 0 interrupt is enabled.

Bits 1,0 – COMPx Comparator x Interrupt Enable
Reading this bit returns the state of the Comparator x interrupt enable.

Writing a '0' to this bit has no effect.

Writing a '1' to this bit will set the Ready interrupt bit and enable the Ready interrupt.

Value	Description
0	The Comparator x interrupt is disabled.
1	The Comparator x interrupt is enabled.

49.8.8 Debug control

Name: DBGCTRL
Offset: 0x1E
Reset: 0x00
Property: PAC Write-Protection

Bit	7	6	5	4	3	2	1	0
						FDDBD		DBGRUN
Access						R/W		R/W
Reset						0		0

Bit 2 – FDDBD Fault Detection on Debug Break Detection
This bit is not affected by software reset and should not be changed by software while the TCC is enabled.

By default this bit is zero, and the on-chip debug (OCD) fault protection is disabled. When this bit is written to '1', OCD break request from the OCD system will trigger non-recoverable fault. When this bit is set, OCD fault protection is enabled and OCD break request from the OCD system will trigger a non-recoverable fault.

Value	Description
0	No faults are generated when TCC is halted in debug mode.
1	A non recoverable fault is generated and FAULTD flag is set when TCC is halted in debug mode.

Bit 0 – DBGRUN Debug Running State
This bit is not affected by software reset and should not be changed by software while the TCC is enabled.

Value	Description
0	The TCC is halted when the device is halted in debug mode.
1	The TCC continues normal operation when the device is halted in debug mode.