ARM®

PrimeCell® Infrastructure AMBA™ 3 AXI™ TrustZone™ Memory Adapter (BP141)
Revision: r0p0
Technical Overview

This technical overview describes the functionality of the PrimeCell Infrastructure AMBA 3 AXI *TrustZone Memory Adapter* (TZMA) in the following sections:

1 Preliminary material

1.1 Release information

Changes to this document are listed in Table 1.

Table 1 Change history

Date	Issue	Change
16 December 2004	A	First issue for r0p0

1.2 Proprietary notice

1.3 Confidentiality status

1.4 Product status

The information in this document is for an final product, that is a developed product.

1.5 Web address

`http://www.arm.com`

2 About the AXI TrustZone memory adapter

The TZMA, `TZMemAdapAxi`, is an AMBA-compliant, SoC peripheral that is developed, tested, and licensed by ARM Limited.

At SoC design time, it is unlikely that the relative requirements of on-chip secure versus non-secure RAM capacity are known. A SoC design that forces fixed partitioning between these RAM areas is likely to lead to an inefficient or inadequate implementation in different security applications. The TZMA solves this problem by enabling a single physical memory cell of up to 2MB to be shared between a secure and non-secure storage area. The partitioning between these areas is flexible.

The TZMA routes transactions according to:

- the memory region that they are attempting to access
- their security mode.

Non-secure accesses to the secure region and accesses to beyond the maximum addressed memory size are cancelled by sending an AXI DECERR response to the originating master. All other transactions are passed from the slave interface to the master interface.

The TZMA has the following features:

- it is compatible with the AXI internal memory interface (BP140)
- it has configuration inputs that can be driven from the *TrustZone Protection Controller* (TZPC) or tied off as required.
- it supports both a single active read and a single active write transaction
- it does not have an AXI low-power interface because it does not initiate transfers or have a power-down sequence
- it does not provide exclusive access monitoring
- you can configure the following parameters:
  - data width of 64 bits or 32 bits
  - ID width, the default is four bits
  - addressed memory size of up to 2MB
- the HDL code is supplied as Verilog.

Figure 1 on page 5 shows a TZMA configured in a typical TrustZone-enabled design.

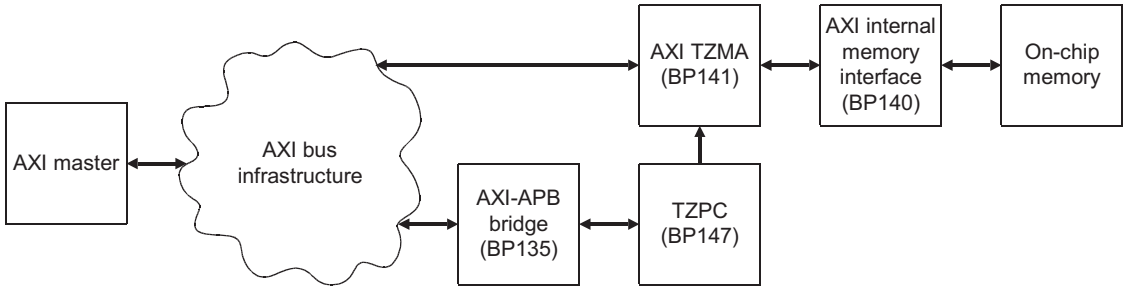

Figure 1 Typical configuration

The other components shown in Figure 1 are:

AXI master This initiates read and write transactions.

AXI bus infrastructure

This is typically a bus matrix or interconnect. You can use the PrimeCell Configurable AXI Interconnect (PL300) to implement this.

AXI-APB bridge

This connects between the AXI and APB domains.

TZPC This provides a software interface to set up memory areas as secure or non-secure.

AXI Memory Interface

This provides a single-port memory interface that you can configure for your on-chip memory.

3 Functional description

The TZMA is described in:

- *Functional blocks*
- *Interface attributes* on page 7.

3.1 Functional blocks

Figure 2 shows a functional block diagram of the TZMA. It contains the sub-blocks described in:

- *Write channel router*
- *Read channel router* on page 7
- *Address comparator* on page 7.

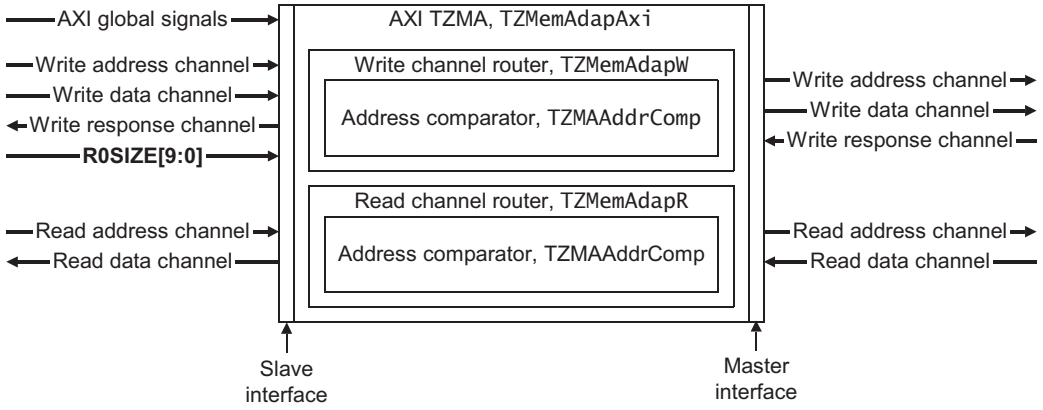

Figure 2 AXI TrustZone memory adapter

Write channel router

Transactions presented at the AXI slave interface are checked against the current security configuration. If a transaction passes this security check then it is routed through to the AXI master interface. If it fails then it is rejected by routing to an internal default slave that generates **BVALID** and signals DECERR on **BRESP**.

One write transaction is handled at a time. Further transactions are held off until outstanding transactions are completed. If there are no other transactions in progress then routing is set up as soon as **AWVALID** is asserted so that no unnecessary latency is introduced.

Read channel router

This operates in a similar manner to the write channel router. If an illegal transaction is detected then an internal default slave signals **RVALID** and generates a DECERR response on **RRESP**.

Address comparator

This compares the input address and transaction protection information against the secure region size from the configuration inputs and the addressed memory size. It uses this information to determine if the address is legal.

3.2 Interface attributes

The master and slave interface attributes for the TZMA are described in Table 2 and Table 3 on page 8.

Table 2 Master interface attributes

Attribute	Description	Value
Write issuing capability	The maximum number of active write transactions that a master can generate	1
Read issuing capability	The maximum number of active read transactions that a master can generate	1
Write ID capability	The maximum number of different **AWID** values that a master can generate for all active write transactions at any one time	1
Write ID width	The number of bits in the **AWID** and **WID** buses	Set by the `ID_WIDTH` parameter
Read ID capability	The maximum number of different **ARID** values that a master can generate for all active read transactions at any one time	1
Read ID width	The number of bits in the **ARID** bus	Set by the `ID_WIDTH` parameter

Table 3 Slave interface attributes

Attribute	Description	Value
Write acceptance capability	The maximum number of active write transactions that a slave can accept.	1
Read acceptance capability	The maximum number of active read transactions that a slave can accept.	1
Write interleave depth	The number of active write transactions for which the slave can receive data. It is counted from the earliest transaction.	1
Read data reorder depth	The number of active read transactions for which a slave may transmit data. It is counted from the earliest transaction.	1

4 Physical data

This section describes:

- *AC characteristics*
- *Gate count*.

4.1 AC characteristics

The TZMA conforms to the AMBA AXI timing parameters. The figures refer to the percentage of clock cycle allowed for each function:

- AXI inputs must be valid for 30% prior to the rising edge of the clock
- AXI outputs must be valid for 20% after the rising edge of the clock
- AXI-AXI combinatorial path delay for approximately 20% of the clock cycle

Note

The timing figures assume that:

- the **R0SIZE** configuration inputs are driven from an APB slave
- the APB clock frequency is half of AXI.

Timing characteristics are confirmed by performing synthesis on the block using the slow-slow process point of the Artisan SAGE HS library for the TSMC CL013G process at a target speed of 200MHz.

4.2 Gate count

Table 4 lists the estimated total gate counts for the library described in *AC characteristics*.

Table 4 Estimated gate counts

Data width	NAND2x1 equivalents
64	560
32	530

Note

The gate count estimates do not include scan logic.

5 Signal descriptions

Figure 3 shows the signal connections.

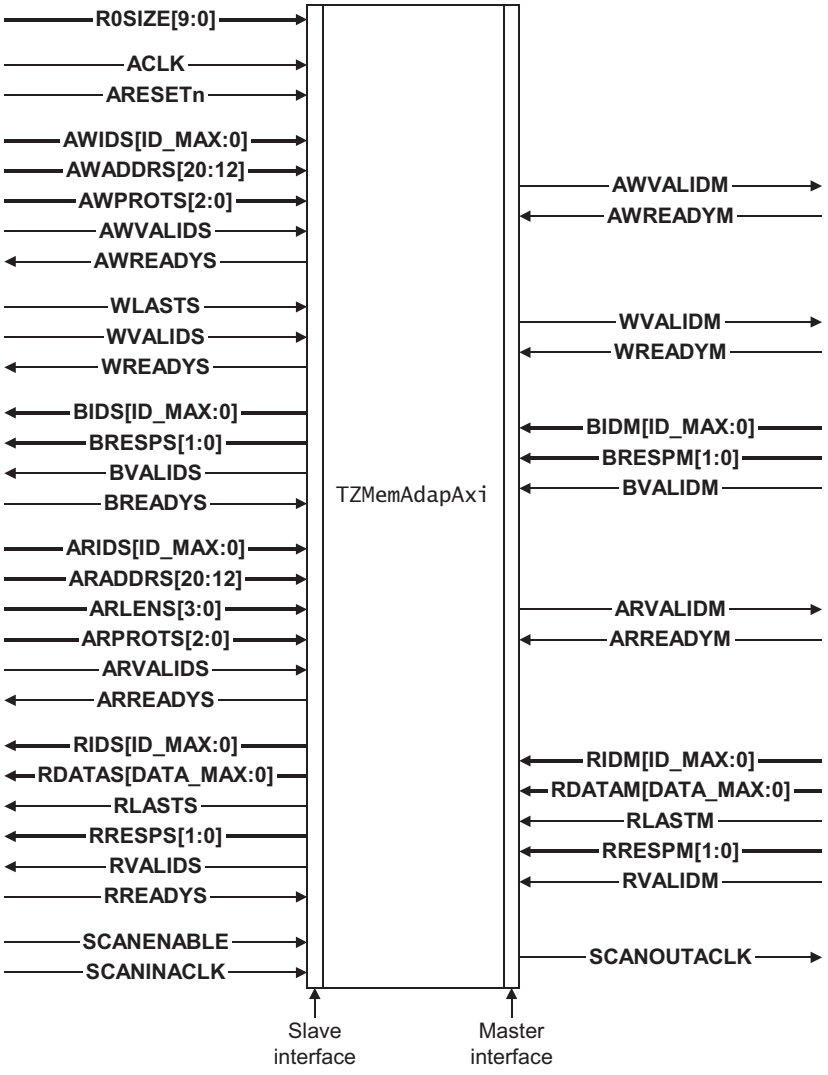

Figure 3 TZMA signal connections

Note

In Figure 3 on page 10:

- AXI signals that are not present on the slave and master interfaces bypass the TZMA.
- The read channel and write channel signals are appended with:
  - the letter M for signals that connect to the component master interface
  - the letter S for signals that connect to the component slave interface.
- The upper value of some bus widths is provided as a name to indicate that the number of signal lines in the bus is derived from user-defined generics or parameters. The *PrimeCell Infrastructure AMBA 3 AXI TrustZone Memory Adapter (BP141) Design Manual* describes these.

The TZMA signals are described in:

- *AMBA AXI signals*
- *Non-AMBA signals*.

5.1 AMBA AXI signals

The *AMBA AXI Protocol Specification* describes the AMBA AXI signals that the TZMA uses.

5.2 Non-AMBA signals

The non-AMBA signals are described in:

- *Secure memory region size*
- *Scan test* on page 12.

Secure memory region size

The **R0SIZE[9:0]** input is derived from the TZPC. It provides the secure memory region size to the TZMA. See the *PrimeCell Infrastructure AMBA 3 TrustZone Protection Controller (BP147) Technical Overview* for more information.

Scan test

Table 5 lists the TZMA internal scan test control signals.

Table 5 Scan test control signals

Name	Type	Source/destination	Description
SCANENABLE	Input	Scan controller	Scan enable, for all clock domains
SCANINACLK	Input	Scan controller	Scan data input for **ACLK** domain
SCANOUTACLK	Output	Scan controller	Scan data output for **ACLK** domain