

ON Semiconductor

Is Now

onsemi™

To learn more about onsemi™, please visit our website at
www.onsemi.com

onsemi and **onsemi** and other names, marks, and brands are registered and/or common law trademarks of Semiconductor Components Industries, LLC dba "**onsemi**" or its affiliates and/or subsidiaries in the United States and/or other countries. **onsemi** owns the rights to a number of patents, trademarks, copyrights, trade secrets, and other intellectual property. A listing of **onsemi** product/patent coverage may be accessed at www.onsemi.com/site/pdf/Patent-Marking.pdf. **onsemi** reserves the right to make changes at any time to any products or information herein, without notice. The information herein is provided "as-is" and **onsemi** makes no warranty, representation or guarantee regarding the accuracy of the information, product features, availability, functionality, or suitability of its products for any particular purpose, nor does **onsemi** assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation special, consequential or incidental damages. Buyer is responsible for its products and applications using **onsemi** products, including compliance with all laws, regulations and safety requirements or standards, regardless of any support or applications information provided by **onsemi**. "Typical" parameters which may be provided in **onsemi** data sheets and/or specifications can and do vary in different applications and actual performance may vary over time. All operating parameters, including "Typicals" must be validated for each customer application by customer's technical experts. **onsemi** does not convey any license under any of its intellectual property rights nor the rights of others. **onsemi** products are not designed, intended, or authorized for use as a critical component in life support systems or any FDA Class 3 medical devices or medical devices with a same or similar classification in a foreign jurisdiction or any devices intended for implantation in the human body. Should Buyer purchase or use **onsemi** products for any such unintended or unauthorized application, Buyer shall indemnify and hold **onsemi** and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, and expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that **onsemi** was negligent regarding the design or manufacture of the part. **onsemi** is an Equal Opportunity/Affirmative Action Employer. This literature is subject to all applicable copyright laws and is not for resale in any manner. Other names and brands may be claimed as the property of others.



AX8052 Cryptographic Functions Programming Manual

Introduction

AX8052 features cryptographic hardware, namely a True Random Number Generator (RNG) and a high speed Advanced Encryption Standard (AES) encryption/decryption engine.

The True Random Number Generator produces, after postprocessing, cryptographic quality random numbers that pass the NIST Statistical Test Suite for Random Number Generators.

The AES engine supports AES-128, AES-192 and AES-256 international standards, as well as programmable round numbers and software key schedule generation to allow longer key lengths for higher security applications. It supports ECB, CFB and OFB chaining modes directly in hardware. Multi-Megabit/s data rates can be achieved thanks to the dedicated DMA controller that reads input data and the keystream directly from X RAM and stores output data into X RAM.

APPLICATION NOTE

A software support library, libmfcrypto, software support routines, such as AES keystream expansion, as well as additional, software-only, algorithms, such as DES.

Address Space

For a description of the AX8052 memory architecture and address spaces, please refer to the AX8052 Family Programming Manual.

Table 1. X REGISTER ADDRESS MAP

Address Hex	Register							
	0	1	2	3	4	5	6	7
	8	9	A	B	C	D	E	F
0x7080 – 0x708F	RNGMODE	RNGBYTE	RNGCLKSRC0	RNGCLKSRC1	–	–	–	–
	–	–	–	–	–	–	–	–
0x7090 – 0x709F	AESMODE	AESCONFIG	AESKEYADDR0	AESKEYADDR1	AESINADDR0	AESINADDR1	AESOUTADDR0	AESOUTADDR1
	AESCURBLO CK	–	–	–	–	–	–	–

Table 2. REGISTER OVERVIEW

Add Hex	Name	Dir	R	Reset	Bit								Description
					7	6	5	4	3	2	1	0	
Random Number Generator													
7080	RNGMODE	RW	R	----1110	RNG AVAIL	–	–	–	–	RNGENTROPY(2:0)		RNG IRQ EN	Random Number Generator Mode
7081	RNGBYTE	R	R	-----	RNGBYTE(7:0)								Random Byte
7082	RNGCLKSRC0	RW	R	--001111	–	–	RNGCLKDIV0(2:0)		RNGCLKSRC0(2:0)		Random Number Generator Clock Source 0		
7083	RNGCLKSRC1	RW	R	---00111	–	–	RNGCLKDIV1(2:0)		RNGCLKSRC1(2:0)		Random Number Generator Clock Source 1		
AES													
7090	AESMODE	RW	R	00000000	AES RUN	AES INV	AESCOUNT(5:0)					AES Mode	
7091	AESCONFIG	RW	R	00001010	AESMODE(1:0)		AESROUNDS(5:0)					AES Cipher Configuration	
7092	AESKEYADDR0	RW	R	00000000	AESKEYADDR(7:0)							AES Keystream Buffer Address	

Table 2. REGISTER OVERVIEW

Add Hex	Name	Dir	R	Reset	Bit								Description
					7	6	5	4	3	2	1	0	
7093	AESKEYADDR1	RW	R	00000000	AESKEYADDR(15:8)								AES Keystream Buffer Address
7094	AESINADDR0	RW	R	00000000	AESINADDR(7:0)								AES Input Buffer Address
7095	AESINADDR1	RW	R	00000000	AESINADDR(15:8)								AES Input Buffer Address
7096	AESOUTADDR0	RW	R	00000000	AESOUTADDR(7:0)								AES Output Buffer Address
7097	AESOUTADDR1	RW	R	00000000	AESOUTADDR(15:8)								AES Output Buffer Address
7098	AESCURBLOCK	R	R	-----	AES RUN	-	AESCURBLOCK(5:0)					AES Current Block	

Random Number Generator

The Random Number Generator uses on-chip noise sources to generate a string of random bits. This is in contrast to pseudo-random number generators often used, which only look random but are in fact generated by a deterministic algorithm.

The output of the Random Number Generator passes the FIPS Test Suite. For high security applications, bits from the RNGBYTE should not be used directly, however, because

each bit provides only slightly less than one bit entropy. Bits should be fed however into an entropy pool first.

The recommended settings are:

Table 3.

Register	Value
RNGMODE	0x0F
RNGCLKSRC0	0x09
RNGCLKSRC1	0x00

Table 4. REGISTER: RNGMODE

Name	Bits	R/W	Reset	Description																		
RNGIRQEN	0	RW	0	Random Number Generator Interrupt Enable																		
RNGENTROPY	3:1	RW	111	Entropy assumed to be within one input bit <table border="0"> <tr> <td>Bits</td> <td>Meaning</td> </tr> <tr> <td>000</td> <td>1 Bit</td> </tr> <tr> <td>001</td> <td>1/2 Bit</td> </tr> <tr> <td>010</td> <td>1/4 Bit</td> </tr> <tr> <td>011</td> <td>1/8 Bit</td> </tr> <tr> <td>100</td> <td>1/16 Bit</td> </tr> <tr> <td>101</td> <td>1/32 Bit</td> </tr> <tr> <td>110</td> <td>1/64 Bit</td> </tr> <tr> <td>111</td> <td>1/128 Bit</td> </tr> </table>	Bits	Meaning	000	1 Bit	001	1/2 Bit	010	1/4 Bit	011	1/8 Bit	100	1/16 Bit	101	1/32 Bit	110	1/64 Bit	111	1/128 Bit
Bits	Meaning																					
000	1 Bit																					
001	1/2 Bit																					
010	1/4 Bit																					
011	1/8 Bit																					
100	1/16 Bit																					
101	1/32 Bit																					
110	1/64 Bit																					
111	1/128 Bit																					
RNGAVAIL	7	R	-	When 1, a random byte is available in RNGBYTE; this bit is cleared by reading RNGBYTE																		

Table 5. REGISTER: RNGBYTE

Name	Bits	R/W	Reset	Description
RNGBYTE	7:0	R	-	Random Byte

AND9477/D

Table 6. REGISTER: RNGCLKSRC0

Name	Bits	R/W	Reset	Description
RNGCLKSRC0	2:0	RW	111	Clock Source Bits Meaning 000 FRCOSC 001 LPOSC 010 XOSC 011 LPXOSC 100 RSYCLK 101 T0CLK 110 System Clock 111 Off
RNGCLKDIV0	5:3	RW	001	Clock Prescaler Bits Meaning 000 × 2 001 × 1 010 ÷ 2 011 ÷ 4 100 ÷ 8 101 ÷ 16 110 ÷ 32 111 ÷ 64

Table 7. REGISTER: RNGCLKSRC1

Name	Bits	R/W	Reset	Description
RNGCLKSRC1	2:0	RW	111	Clock Source Bits Meaning 000 FRCOSC 001 LPOSC 010 XOSC 011 LPXOSC 100 RSYCLK 101 T0CLK 110 System Clock 111 Off
RNGCLKDIV1	5:3	RW	000	Clock Prescaler Bits Meaning 000 ÷ 1 001 ÷ 2 010 ÷ 4 011 ÷ 8 100 ÷ 16 101 ÷ 32 110 ÷ 64 111 ÷ 128

AND9477/D

AES

The AES Block implements the government mandated Advanced Encryption Standard (AES) encryption algorithm data path. It offers a programmable round number, a programmable number of 16 Byte blocks and the ECB, CFB and OFB modes are directly implemented in hardware.

It encrypts or decrypts a buffer in X memory into a buffer in X memory. Since it features 16 bit wide datapaths into X

memory, it is recommended that its buffers be even address aligned. A small performance penalty results from using odd address aligned buffers.

The key schedule must be precomputed in software and stored in a keystream buffer (up to about 256 Bytes) somewhere in X memory.

Table 8. REGISTER: AESMODE

Name	Bits	R/W	Reset	Description
AESCOUNT	5:0	RW	000000	AES Input/Output Buffer Length (number of 16 Byte or 128 Bit AES Blocks)
AESINV	6	RW	0	AES Mode; 0 = encrypt, 1 = decrypt
AESRUN	7	RW	0	AES Run; writing 1 starts encryption/decryption

Table 9. REGISTER: AESCONFIG

Name	Bits	R/W	Reset	Description										
AESROUNDS	5:0	RW	001010	Number of Rounds; usually 10 for AES-128, 12 for AES-192 and 14 for AES-256										
AESMODE	7:6	RW	00	AES Cipher Chaining Mode <table border="0"> <tr> <td>Bits</td> <td>Meaning</td> </tr> <tr> <td>00</td> <td>ECB (Electronic Codebook)</td> </tr> <tr> <td>01</td> <td>invalid</td> </tr> <tr> <td>10</td> <td>CFB (Cipher Feedback)</td> </tr> <tr> <td>11</td> <td>OFB (Output Feedback)</td> </tr> </table>	Bits	Meaning	00	ECB (Electronic Codebook)	01	invalid	10	CFB (Cipher Feedback)	11	OFB (Output Feedback)
Bits	Meaning													
00	ECB (Electronic Codebook)													
01	invalid													
10	CFB (Cipher Feedback)													
11	OFB (Output Feedback)													

Table 10. REGISTER: AESKEYADDR0, AESKEYADDR1

Name	Bits	R/W	Reset	Description
AESKEYADDR	15:0	RW	0x0000	X Space Address of the Keystream Buffer

Table 11. REGISTER: AESINADDR0, AESINADDR1


Name	Bits	R/W	Reset	Description
AESINADDR	15:0	RW	0x0000	X Space Address of the Input Buffer

Table 12. REGISTER: AESOUTADDR0, AESOUTADDR1

Name	Bits	R/W	Reset	Description
AESOUTADDR	15:0	RW	0x0000	X Space Address of the Output Buffer

Table 13. REGISTER: AESCURBLOCK

Name	Bits	R/W	Reset	Description
AESCURBLOCK	5:0	R	-	Current Block (16 Byte, 128 Bit chunk); Processing starts at 1 and ends at AESCOUNT
AESRUN	7	R	-	AES Run; 1 means encryption/decryption ongoing, 0 means idle

ON Semiconductor and  are trademarks of Semiconductor Components Industries, LLC dba ON Semiconductor or its subsidiaries in the United States and/or other countries. ON Semiconductor owns the rights to a number of patents, trademarks, copyrights, trade secrets, and other intellectual property. A listing of ON Semiconductor's product/patent coverage may be accessed at www.onsemi.com/site/pdf/Patent-Marking.pdf. ON Semiconductor reserves the right to make changes without further notice to any products herein. ON Semiconductor makes no warranty, representation or guarantee regarding the suitability of its products for any particular purpose, nor does ON Semiconductor assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation special, consequential or incidental damages. Buyer is responsible for its products and applications using ON Semiconductor products, including compliance with all laws, regulations and safety requirements or standards, regardless of any support or applications information provided by ON Semiconductor. "Typical" parameters which may be provided in ON Semiconductor data sheets and/or specifications can and do vary in different applications and actual performance may vary over time. All operating parameters, including "Typicals" must be validated for each customer application by customer's technical experts. ON Semiconductor does not convey any license under its patent rights nor the rights of others. ON Semiconductor products are not designed, intended, or authorized for use as a critical component in life support systems or any FDA Class 3 medical devices or medical devices with a same or similar classification in a foreign jurisdiction or any devices intended for implantation in the human body. Should Buyer purchase or use ON Semiconductor products for any such unintended or unauthorized application, Buyer shall indemnify and hold ON Semiconductor and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, and expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that ON Semiconductor was negligent regarding the design or manufacture of the part. ON Semiconductor is an Equal Opportunity/Affirmative Action Employer. This literature is subject to all applicable copyright laws and is not for resale in any manner.

PUBLICATION ORDERING INFORMATION

LITERATURE FULFILLMENT:

Literature Distribution Center for ON Semiconductor
19521 E. 32nd Pkwy, Aurora, Colorado 80011 USA
Phone: 303-675-2175 or 800-344-3860 Toll Free USA/Canada
Fax: 303-675-2176 or 800-344-3867 Toll Free USA/Canada
Email: orderlit@onsemi.com

N. American Technical Support: 800-282-9855 Toll Free
USA/Canada
Europe, Middle East and Africa Technical Support:
Phone: 421 33 790 2910
Japan Customer Focus Center
Phone: 81-3-5817-1050

ON Semiconductor Website: www.onsemi.com
Order Literature: <http://www.onsemi.com/orderlit>
For additional information, please contact your local
Sales Representative