Cryptographic Functions Programming Manual

AX8052 Cryptographic Functions

ON Semiconductor®

TABLE OF CONTENTS

1. 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.

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

2. Acronyms and Abbreviations

AX8052	MCU 8052

3. Address space

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

3.1 X REGISTER ADDRESS MAP

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

3.2 REGISTER OVERVIEW

Addr	Name	Dir	R	Reset	Bit								Description
Hex					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	——000111	–	–	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

Addr	Name	Dir	R	Reset	Bit							
Hex					7	6	5	4	3	2	1	0
7091	AESCONFIG	RW	R	00001010	AESCMODE(1:0)		AESROUNDS(5:0)					
7092	AESKEYADDR0	RW	R	00000000	AESKEYADDR(7:0)							
7093	AESKEYADDR1	RW	R	00000000	AESKEYADDR(15:8)							
7094	AESINADDR0	RW	R	00000000	AESINADDR(7:0)							
7095	AESINADDR1	RW	R	00000000	AESINADDR(15:8)							
7096	AESOUTADDR0	RW	R	00000000	AESOUTADDR(7:0)							
7097	AESOUTADDR1	RW	R	00000000	AESOUTADDR(15:8)							
7098	AESCURBLOCK	R	R	————	AES RUN	–	AESCURBLOCK(5:0)					

4. 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:

Register	**Value**
RNGMODE	0x0F
RNGCLKSRC0	0x09
RNGCLKSRC1	0x00

4.1 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 Bits Meaning 000 1 Bit 001 $\frac{1}{2}$ Bit 010 $\frac{1}{4}$ Bit 011 $\frac{1}{8}$ Bit 100 $\frac{1}{16}$ Bit 101 $\frac{1}{32}$ Bit 110 $\frac{1}{64}$ Bit 111 $\frac{1}{128}$ Bit
RNGAVAIL	7	R	–	When 1, a random byte is available in RNGBYTE; this bit is cleared by reading RNGBYTE

4.2 Register : RNGBYTE

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

4.3 Register : RNGCLKSRC0

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

4.4 Register : RNGCLKSRC1

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

5. 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.

5.1 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

5.2 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
AESCMODE	7:6	RW	00	AES Cipher Chaining Mode Bits | Meaning 00 | ECB (Electronic Codebook) 01 | invalid 10 | CFB (Cipher Feedback) 11 | OFB (Output Feedback)

5.3 Register : *AESKEYADDR0*, AESKEYADDR1

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

5.4 Register : AESINADDR0, AESINADDR1

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

5.5 Register : AESOUTADDR0, AESOUTADDR1

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

5.6 Register : AECCURBLOCK

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

6. HISTORY

Version	Date	Comments
1.0		Added AX8052 Crypto programming manual details
1.1	12-Feb-2019	Format changes

7. Contact Information

ON Semiconductor
Oskar-Bider-Strasse 1
CH-8600 Dübendorf
SWITZERLAND

Phone +41 44 882 17 07
Fax +41 44 882 17 09
Email sales@onsemi.com
www.onsemi.com

For further product related or sales information please visit our website or contact your local representative.

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.