Random Number Generation Using MSP430™ MCUs

MSP430 Applications

ABSTRACT

Many applications require the generation of random numbers. These random numbers are useful for applications such as communication protocols, cryptography, and device individualization.

Generating random numbers often requires the use of expensive dedicated hardware. Using the two independent clocks available on the MSP430F2xx family of devices, software can generate random numbers without such hardware.

Source files for the software described in this application report can be downloaded from http://www.ti.com/lit/zip/slaa338.

Contents

Trademarks

MSP430 is a trademark of Texas Instruments.
All other trademarks are the property of their respective owners.

1 Introduction

The very-low-frequency oscillator (VLO) and digitally controlled oscillator (DCO) are two independent clock systems, each having its own timing source. Because the clocks are independent, the time difference between edge transitions of these two clock sources varies. The timing differences between these two clock systems can be exploited to generate a stream of random bits. In one VLO clock cycle, there are always approximately the same number of DCO pulses. However, because the two clock sources vary independently from each other, whether this number of pulses is even or odd is not predictable. More importantly, this number is not predictable even if the previous result is known.

Therefore, Timer_A can be configured to continuously count the number of DCO clock cycles per VLO clock cycle, and the least-significant bits (LSBs) from 16 of these results can be concatenated to form a random 16-bit integer.

2 Setup

Timer_A is configured in capture mode. SMCLK is sourced from the DCO and set as the input clock to Timer_A. ACLK is sourced from the VLO, which is the trigger for the capture. Timer_A counts the number of DCO clock pulses before the next VLO low-to-high transition occurs. The number of DCO clock pulses is saved by the timer in a capture/compare register (CCR). The LSB from the CCR is saved by left shifting it into a CPU register (R12). This process is repeated until 16 LSBs have been saved, forming a 16-bit result that is almost random.

3 Adding Randomness

The example software included also takes several measures that are designed to increase the randomness of the numbers measured and to make the overall system less predictable.

- Each time a CCR LSB is shifted, the BCSCTL1 register has the number five added to it. This addition changes the RSEL bits, causing the DCO speed to change relative to the VLO through each loop. Although any number could be used, testing showed that five caused a large enough step change to significantly vary the DCO with respect to the VLO.
- Each time a CCR LSB is shifted, the two LSBs from the R12 register are XORed into the DIVA bits of the BCSCTL1. The DIVA bits control the divider used for the VLO before it reaches the timer. This also changes the relationship between the VLO and DCO as measured by the timer.
- Each result bit is actually the result of a majority vote of five loops. Each loop generates its own LSB from the CCR as described earlier, but the majority vote of five is used to select the final resultant bit. This majority vote system more evenly distributes the results and causes them to pass the poker test for randomness as described in Section 6.

4 Usage

Section 3 describes methods that add randomness, and Section 6 describes how these methods have been tested to more evenly distribute the resultant data. These methods do, however, make changes to the clock system of the MSP430™ MCU, which could interfere with other running processes. Such considerations should be made when designing a system.

If such clock-system changes are not acceptable for a running application, it still may be possible to make use of the methods presented in this application report. Instead of using these methods each time a random number is desired, an initial seed could be generated. This seed value would use these methods, and do so at device startup, before any other processes that rely on the clock system have begun. This seed could be used as a seed for a pseudo-random number generation (PRNG) algorithm such as a steam cipher.[1] This method, although more CPU intensive, could also yield numbers with good random properties, depending on the PRNG used.

5 Overview

Figure 1 shows the flow of the software included with this application report.

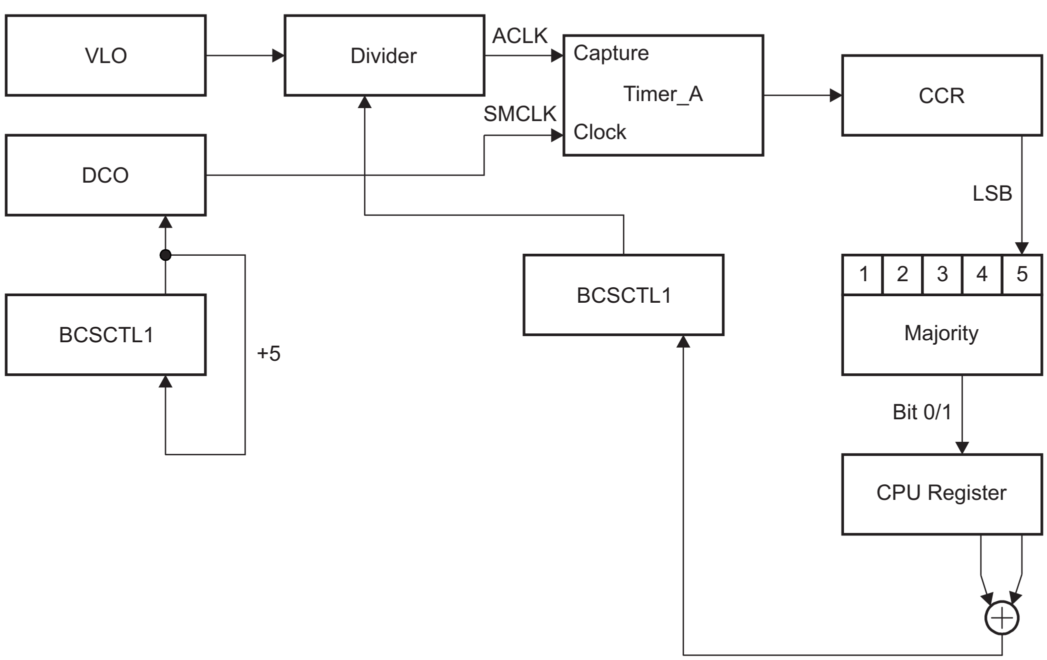

Figure 1. Software Overview Block Diagram

6 Testing for Randomness

The Federal Information Processing Standards (FIPS) describe a series of statistical tests for randomness. Included with the source code for this random number generator is a C file called fips_test.c. This source code implements the FIPS 140-2 tests for randomness. The results of these tests are saved in global variables and can be viewed with a debugger to verify the functionality of the random number generator.

Although the tests are included for statistical information, this application report has not undergone official FIPS certification or testing.

The methods described in this application report make use of timing differences between ACLK and SMCLK in the MSP430 MCU. The VLO was chosen for its device-to-device variation and drift with temperature and voltage. This drift only adds to the observed entropy, and sufficiently random numbers are generated under constant temperature and voltage conditions. These factors also add to the randomness that is observed between devices.

The FIPS 140-2 test is only a necessary requirement for the random numbers generated here. For an application that requires cryptographic secure random numbers, it is necessary to create a model of the system and evaluate the entropy that is generated.[2]

The IEEE paper Analysis of Random Number Generator from Texas Instruments in MSP430x5xx Families provides a more in-depth analysis of the randomness of the generator discussed in this document.

7 LFXT1 and VLO

ACLK could also be sourced from LFXT1 with a 32-kHz crystal. This method can also be used to generate random numbers, but it is less reliable, because of the more predictable nature of the 32-kHz crystal. It is also less secure, because one of the clock sources is now sourced into the microcontroller externally. This fact could be used by an attacker looking to influence the selection of random numbers and compromise a system. These facts should be weighed against the security requirements of a system when deciding to use LFXT1 as the ACLK source for random number generation.

8 References

1. U. Kaiser, Hermes8: A Low-Complexity Low-Power Stream Cipher
2. W. Schindler, Evaluation Criteria for True (Physical) Random Number Generators Used in Cryptographic Applications, CHES2002 workshop
3. MSP430x2xx Family User's Guide
4. MSP430x1xx Family User's Guide
5. FIPS PUB 140-2, National Institute of Standards and Technology
6. Analysis of Random Number Generator from Texas Instruments in MSP430x5xx Families

Revision History

NOTE: Page numbers for previous revisions may differ from page numbers in the current version.

Changes from October 13, 2006 to May 16, 2018	Page
• Editorial changes throughout document	1
• Added link to related IEEE paper as the last paragraph of Section 6, *Testing for Randomness*	3

IMPORTANT NOTICE FOR TI DESIGN INFORMATION AND RESOURCES

Texas Instruments Incorporated ('TI") technical, application or other design advice, services or information, including, but not limited to, reference designs and materials relating to evaluation modules, (collectively, "TI Resources") are intended to assist designers who are developing applications that incorporate TI products; by downloading, accessing or using any particular TI Resource in any way, you (individually or, if you are acting on behalf of a company, your company) agree to use it solely for this purpose and subject to the terms of this Notice.

TI's provision of TI Resources does not expand or otherwise alter TI's applicable published warranties or warranty disclaimers for TI products, and no additional obligations or liabilities arise from TI providing such TI Resources. TI reserves the right to make corrections, enhancements, improvements and other changes to its TI Resources.

You understand and agree that you remain responsible for using your independent analysis, evaluation and judgment in designing your applications and that you have full and exclusive responsibility to assure the safety of your applications and compliance of your applications (and of all TI products used in or for your applications) with all applicable regulations, laws and other applicable requirements. You represent that, with respect to your applications, you have all the necessary expertise to create and implement safeguards that (1) anticipate dangerous consequences of failures, (2) monitor failures and their consequences, and (3) lessen the likelihood of failures that might cause harm and take appropriate actions. You agree that prior to using or distributing any applications that include TI products, you will thoroughly test such applications and the functionality of such TI products as used in such applications. TI has not conducted any testing other than that specifically described in the published documentation for a particular TI Resource.

You are authorized to use, copy and modify any individual TI Resource only in connection with the development of applications that include the TI product(s) identified in such TI Resource. NO OTHER LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE TO ANY OTHER TI INTELLECTUAL PROPERTY RIGHT, AND NO LICENSE TO ANY TECHNOLOGY OR INTELLECTUAL PROPERTY RIGHT OF TI OR ANY THIRD PARTY IS GRANTED HEREIN, including but not limited to any patent right, copyright, mask work right, or other intellectual property right relating to any combination, machine, or process in which TI products or services are used. Information regarding or referencing third-party products or services does not constitute a license to use such products or services, or a warranty or endorsement thereof. Use of TI Resources may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

TI RESOURCES ARE PROVIDED "AS IS" AND WITH ALL FAULTS. TI DISCLAIMS ALL OTHER WARRANTIES OR REPRESENTATIONS, EXPRESS OR IMPLIED, REGARDING TI RESOURCES OR USE THEREOF, INCLUDING BUT NOT LIMITED TO ACCURACY OR COMPLETENESS, TITLE, ANY EPIDEMIC FAILURE WARRANTY AND ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF ANY THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

TI SHALL NOT BE LIABLE FOR AND SHALL NOT DEFEND OR INDEMNIFY YOU AGAINST ANY CLAIM, INCLUDING BUT NOT LIMITED TO ANY INFRINGEMENT CLAIM THAT RELATES TO OR IS BASED ON ANY COMBINATION OF PRODUCTS EVEN IF DESCRIBED IN TI RESOURCES OR OTHERWISE. IN NO EVENT SHALL TI BE LIABLE FOR ANY ACTUAL, DIRECT, SPECIAL, COLLATERAL, INDIRECT, PUNITIVE, INCIDENTAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES IN CONNECTION WITH OR ARISING OUT OF TI RESOURCES OR USE THEREOF, AND REGARDLESS OF WHETHER TI HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

You agree to fully indemnify TI and its representatives against any damages, costs, losses, and/or liabilities arising out of your non-compliance with the terms and provisions of this Notice.

This Notice applies to TI Resources. Additional terms apply to the use and purchase of certain types of materials, TI products and services. These include; without limitation, TI's standard terms for semiconductor products http://www.ti.com/sc/docs/stdterms.htm), evaluation modules, and samples (http://www.ti.com/sc/docs/sampterms.htm).