American National Standard for Financial Services

ANS X9.82: Part 4–2011

Random Number Generation

Part 4: Random Bit Generator Constructions

Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved: November 11, 2011

American National Standards Institute

Table of Contents

Foreword

The Accredited Standards Committee (ASC) on Financial Services (ANSI X9) has developed several cryptographic standards to protect financial information. Many of these standards require the use of Random Number Generators to generate random and unpredictable cryptographic keys and other critical security parameters. This Standard, *Random Number Generation*, defines techniques for the generation of random numbers that are used when other ASC standards require the use of random numbers for cryptographic purposes.

While the techniques specified in this Standard are designed to generate random numbers, the Standard does not guarantee that a particular implementation is secure. It is the responsibility of the financial institution to put an overall process in place with the necessary controls to ensure that the process is securely implemented. Furthermore, the controls should include the application with appropriate validation tests in order to verify compliance with this Standard.

Approval of an American National Standard requires verification by ASC that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ASC Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made toward their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this Standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken to reaffirm, revise, or withdraw this Standard no later than five years from the date of approval.

Published by

Accredited Standards Committee X9 Incorporated
Financial Industry standards
275 West Street, Suite 107
Annapolis, MD 21401 USA
X9 Online http://www.x9.org

Introduction

NOTE The user's attention is called to the possibility that compliance with this Standard may require the use of an invention covered by patent rights.

By publication of this Standard, no position is taken with respect to the validity of this claim or of any patent rights in connection therewith. The patent holder has, however, filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license. Details may be obtained from the standards developer.

Suggestions for the improvement or revision of this Standard are welcome. They should be sent to the X9 Committee Secretariat, Accredited Standards Committee X9, Inc., Financial Industry Standards, 275 West Street, Suite 107, Annapolis, MD 21401 USA.

This Standard was processed and approved for submittal to ANSI by the Accredited Standards Committee on Financial Services, X9. Committee approval of the Standard does not necessarily imply that all the committee members voted for its approval.

The X9 committee had the following members:
X9 Chairman, Roy DeCicco
Vincent DeSantis, X9 Vice-Chairman
Cynthia Fuller, Executive Director

Organization Represented	**Representative**
[X9 membership to be supplied]	

The X9F subcommittee on Data and Information Security had the following members:
Richard J. Sweeney, Chairman

Organization Represented	**Representative**
[X9F membership to be supplied]	

Under ASC X9 procedures, a working group may be established to address specific segments of work under the ASC X9 Committee or one of its subcommittees. A working group exists only to develop standard(s) or guideline(s) in a specific area and is then disbanded. The individual experts are listed with their affiliated organizations. However, this does not imply that the organization has approved the content of the standard or guideline. (Note: Per X9 policy, company names of non-member participants are listed only if, at time of publication, the X9 Secretariat received an original signed release permitting such company names to appear in print.)

The X9F1 Cryptographic Tool Standards and Guidelines group that developed this part of the Standard had the following members:

Terence Spies, Chairman
Elaine Barker, Project Editor

Organization	**Representative**

Certicom Corporation	Dan Brown
Communications Security Establishment of Canada	Jonathon Hammell
National Institute of Standards and Technology	Elaine Barker
	John Kelsey
National Security Agency	Mary Baisch
	Michael Boyle
NTRU	William Whyte
University Bank	Michael Talley
Voltage	Terence Spies

Random Number Generation
Part 4: Random Bit Generator Constructions

1 Scope

Cryptography and security applications make extensive use of random numbers and random bits. However, the generation of random bits is problematic in many practical applications of cryptography. The purpose of American National Standard (ANS) X9.82 is to specify a standard for the design of random bit generators (RBGs) and to provide methods for converting the random bits to random numbers when required. By matching the security requirements of the application using the random bits with the security claims of the RBG generating those bits, an application can safely use the random bits produced by an RBG conforming to this Standard.

The preceding parts of this Standard have addressed the development of components and base concepts for the construction of RBGs:

- Part 1, *Overview and Basic Principles*, provides definitions of fundamental concepts, such as entropy, randomness, and security strengths, and frames the problem of random bit generation for cryptographic and security applications. Part 1 should be read for a basic understanding of this Standard before reading Part 4.
- Part 2, *Entropy Sources*, provides guidance for developing Approved entropy sources – mechanisms that provide truly unpredictable bits from some nondeterministic process.
- Part 3, *Deterministic Random Bit Generator Mechanisms*, specifies several Deterministic Random Bit Generator (DRBG) mechanisms containing cryptographic algorithms that, when used correctly, are expected to produce bits that are indistinguishable from an ideal random sequence, up to the specified security strength of the instantiation.

Part 4 specifies how Approved RBGs **shall** be constructed, using components from Parts 2 and 3 of the Standard. Part 4 specifies constructions for an RBG, and constructions for building components that are used within those RBG constructions. The information in Part 4 is intended to be combined with the information in the Parts 2 and 3 in order to:

- Construct an RBG with the required security properties that will be compliant with the Standard, and
- Verify that an RBG has been constructed in compliance with the Standard.

The precise structure, design and development of an RBG is outside the scope of this Standard.

2 Conformance

An implementation of an RBG may claim conformance with ANS X9.82 if the following are implemented: a source of entropy bits (e.g., an appropriate entropy source from Part 2), the mandatory requirements of one or more of the Deterministic Random Bit Generator (DRBG) mechanisms specified in Part 3, and the appropriate mandatory requirements of Part 4.

Conformance can be assured by a testing laboratory associated with the Cryptographic Module Validation Program (CMVP) (see http://csrc.nist.gov/cryptval). Although an implementation may claim conformance with the Standard apart from such testing, implementation testing through the CMVP is strongly recommended.