ANSI X9.82 (RNGs)

Elaine Barker
National Institute of Standards and Technology
ebarker@nist.gov
301-975-2911

Changes

- Reorganized into five parts:
  - Part 1: Overview and Basic Principles
  - Part 2: DRBGs Based on Hash Functions
  - Part 3: DRBGs Based on Block Ciphers
  - Part 4: DRBGs Based on Hard Problems
  - Part 5: NRBGs

Changes (contd.)

- Terms, definitions, symbols and abbreviations in the appropriate part

Part 1: Overview and Basic Principles

- General Discussion
  - General Functional Model - needs to be reconciled with the text
  - Top level security requirements
  - RBG functional requirements
- Deterministic RBGs
  - As before; what goes here vs. what goes in Parts 2-4?
  - Added section on the error state (7.2.6)

Part 1 (contd.)

- Non-deterministic RBGs
  - What goes here vs. what goes in Parts 5?
- Place holders
  - Hybrid RNGs
  - Using Multiple RBGs
  - Producing RNs from Random Bits
  - Implementation Issues (general)
  - Testing (general)

Parts 2-4: DRBGs

- Scope for each part
- DRBG discussions - currently same as Part 1
- Types of DRBGs
- Approved DRBGs
  - Error state has been indicated