The Strategy Behind the Proposed Random Number Generation Standard

Paul Timmel
Cryptology Office
Information Assurance Research Group
National Security Agency
19 July 2004

Abstract

- Standard: a point of reference against which something may be compared or analyzed.
- NIST, ANSI X9, and ISO have struggled for years to find a meaningful point of reference for cryptographic randomness.
- The current strategy proposes not one but three points of reference.
- This presentation highlights the strategy itself, because it is as important to determine the effectiveness of the strategy as the success or failure to exhibit it in the standard.

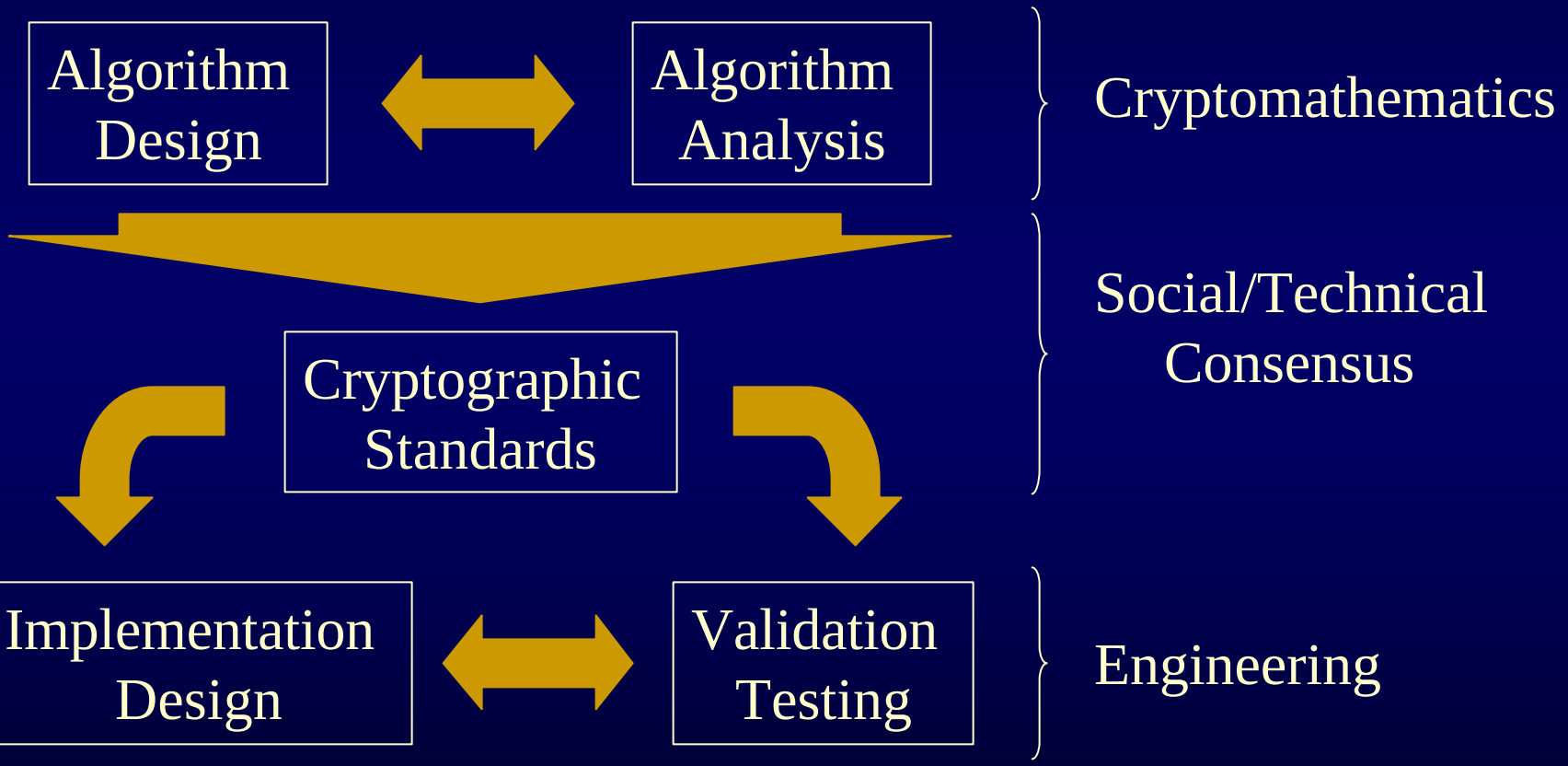
Outline

- Terminology
- The role that standards has acquired in cryptography.
- Cryptographic security dependencies.
- The dilemma about standard RNGs.
- Previous strategies that were considered by NIST, ANSI X9F1, and others.
- The current proposed strategy:
  - Evolved from contributions by NIST and others to X9.82
  - Also being considered for adoption by ISO.

Terminology

- Random Number Generation (RNG)
  - Random bit generation (RBG)
  - Conversion between bit strings and numbers
- Deterministic RBG (DRBG)
  - Pseudo-random output, often called PRNG
  - Algorithmic
- Non-deterministic RBG (NRBG)
  - Truly random output
  - Algorithmic processing of non-deterministic “entropy source”.

Cryptography and Standards



Security, Standards, and Confidence

- Security Standards can:
  - establish grounds for confidence in security products,
  - establish ways to achieve confidence, and
  - guide or bound the confidence required.
- Security and confidence are not synonymous
  - Non-standard products can be secure.
  - Standards-complying products might not be.
- Standards express a consensus about “due diligence” and ease risk assessment.

The Dilemma

- DRBGs
  - Can be standardized like any other algorithm.
  - Are only as good as the random (non-deterministic) seed.
- NRBGs do not admit to complete abstract specification.
  - Standards are meant to be implementation independent.
  - For NRBGs, “the devil is in the [implementation] details.”
- The NRBG details ignored by current standards leave a gap in security arguments.
  - Cryptographic standards assume that secret keys and seeds are suitably random.
  - Without NRBG standards, that assumption cannot be validated in products.

Prior Solution Strategies and Shortcomings

- Statistical Acceptance Tests
- Standardized Designs
- Design Criteria

Statistical Acceptance Tests

- Potential strategy: standardize tests instead of RBGs.
- Test suite examples: NIST, Marsaglia's Diehard.
- Problems
  - Plausible for NRBGs, but can't address DRBGs.
  - Where/how should the tests be applied?
    - To raw digitized entropy?
    - After processing to remove bias, and correlation?
  - Tests are most effective when tailored to design details.
  - Statistics can distinguish between random sequences and predetermined alternatives, but cannot automatically infer what those alternatives should be.
- Statistics is a tool, not a cure-all.

Standard Designs

- Standard designs work for DRBGs.
- Standard designs would make tests meaningful for NRBGs.
- However:
  - Robust entropy sources are implementation and technology specific.
  - Technology may change too fast for a standard design to stay relevant.
  - The critical implementation details are usually proprietary.
  - Is there sufficient literature on NRBGs and entropy sources on which to base standard designs?

Design Criteria

- Criteria would be implementation independent
  - Criteria would establish the grounds for acceptable designs.
  - Criteria would define the evidence that designs and implementations must create to support independent validation and acceptance.
- However:
  - Design/product validation could cost more (time and expertise) than for other approaches.
  - Criteria are most effectively derived from published literature, of which there is little.

Proposed Three-Point Strategy

- Establish abstract criteria for cryptographic RNGs.
- Treat DRBGs as cryptographic algorithms.
  - Evaluate against abstract criteria.
  - Make explicit the dependence on a random seed.
- Treat NRBGs as a combination of an entropy source and some deterministic algorithms.
  - Standardize the deterministic elements as usual.
  - Craft specific design criteria, guidance, and validation methodology for entropy sources.

Part 1: Abstract Criteria

- Establishes a foundation for Parts 2 and 3.
  - Important to at least the standards process to ensure that the other parts are consistent and compatible.
- Establishes what consuming cryptographic algorithms (and standards) can expect from RNGs and how to get it.
  - Consuming algorithms (and security arguments) shouldn’t usually need to distinguish whether keys come from DRBGs or NRBGs.

Part 3: Deterministic RBGs

- Adopts algorithms that meet the criteria of Part 1 (as determined through the consensus of the standards process).
- Presents the algorithms in a consistent framework covering interfaces, seeding, implementation, and validation, so that the algorithms can be functionally interchangeable.

Part 2: Non-Deterministic RBGs

- Establishes the design criteria for entropy sources.
  - These criteria are a specialization of Part 1.
  - Would be used by the standards process to adopt standard designs, if standard designs were practical.
  - Absent standard designs, consumers of RNGs must employ other means to gain confidence that these criteria are met.
- Governs how entropy sources are employed in order to maximize assurance.

Summary

- NIST, working in ANSI X9F1, has developed a three-part strategy for standardizing RNGs.
  - Separate treatment for DRBGs and NRBGs.
  - A unifying foundation of abstract criteria, which is also the basis for interface with other standards.
- During this workshop, as much consideration should be given to the strategy as to the content of the three parts.