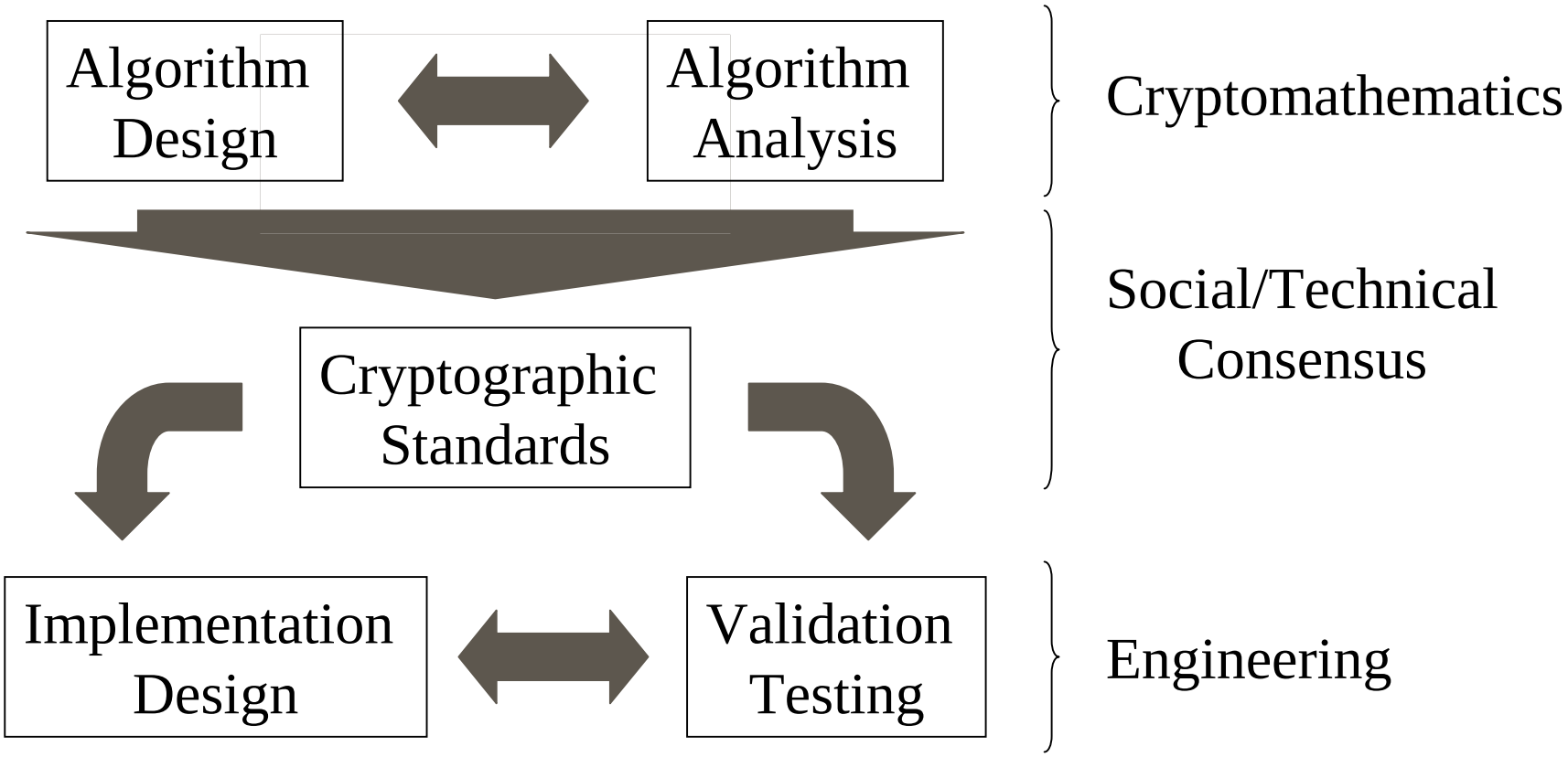
True Random Number Generation: A Standard(s) Dilemma

Paul Timmel
Cryptology Office
Information Assurance Research Group
National Security Agency
24 June 2002

Overview and Thesis

- Cryptography depends on the randomness of secrets and other values (e.g. keys) for security.
- Existing standards either do not address that, or generate them from an initial secret of unspecified provenance.
- ISO, NIST, and ANSI X9 (at least) are finding the problem difficult to address.
- Rigorous literature on true (non-deterministic) random number generators (TRNGs) is scarce.
- TRNGs are an important information assurance frontier that should be rich with opportunities for publication.

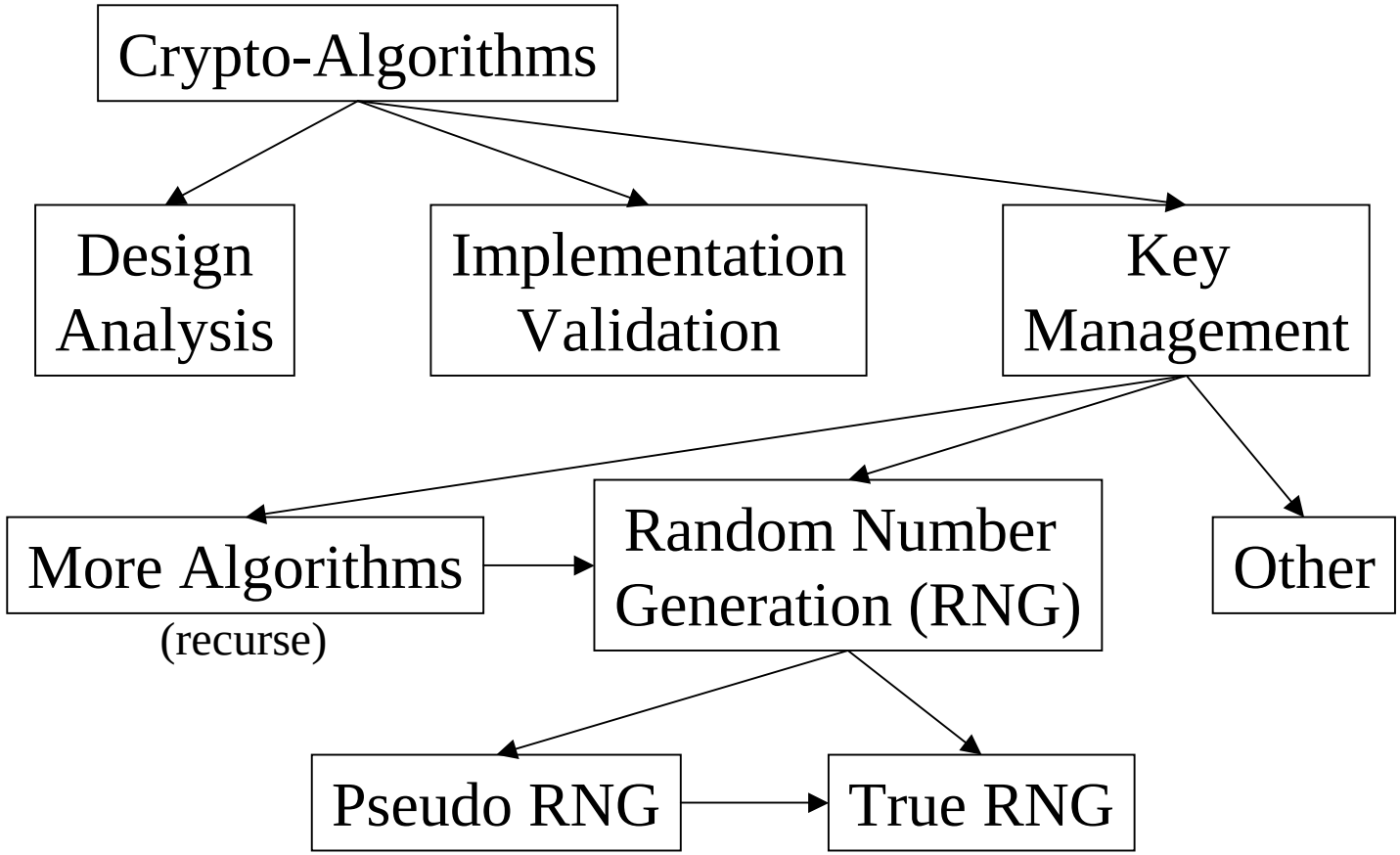
Information Assurance and Standards



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.

Cryptographic Security Dependencies



The Dilemma

- True random number generation (TRNG) does not admit to complete abstract specification.
  - Standards are implementation independent.
  - “The devil is in the [implementation] details.”
- The TRNG details ignored by standards leave a gap in security arguments.
  - Cryptographic standards assume that secret keys and seeds are suitably random.
  - Without TRNG standards, that assumption cannot be completely validated in products.

Solution Strategies and Shortcomings

- Statistical Acceptance Tests
- Standardized Designs
- Design Criteria

Statistical Acceptance Tests

- Examples: Diehard, NIST
- Problems
  - Where/how should the tests be applied?
  - Can’t define a general answer without considering design details.
  - Statistics can distinguish between random sequences and predetermined alternatives, but cannot derive those alternatives.
- Statistics is a tool, not a panacea.

Standard RNG Designs

- Standard designs would make tests meaningful.
- However:
  - Robust TRNG designs are implementation and technology specific.
  - Technology changes too fast for a standard design to stay relevant.
  - The critical implementation details are usually proprietary.
  - There is insufficient literature on TRNGs 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.

Topics Worthy of Exploration

- Entropy Source Identification and Analysis
  - Entropy estimation tools suited for cryptography.
  - Methodology for both low rate and high rate sources.
  - Degenerate conditions and environmental factors.
  - Theory versus practice: technology and environment.
- Implementation Design and Criteria
  - Functional requirements for cryptographic TRNGs.
  - Designing for assurance: a matter of process.
  - Designing for validation: a matter of evidence.

More Topics

- Implementation Validation
  - What to validate: theory, design, product, or all three?
  - How to validate: what to do with the evidence.
  - Levels of assurance: one size won’t fit all.
  - Keeping validation cost-effective.

Summary

- Cryptographic standards rely on but do not yet address TRNGs.
- TRNGs have many open issues concerning both principles and practice.
- These issues have largely escaped rigorous scrutiny.
- Further improvement in cryptographic assurance will likely depend upon pragmatic solutions to these issues.