Empirical Statistical Testing Of Cryptographic PRNGs

Juan Soto

National Institute Of Standards & Technology

soto@nist.gov

Existing Packages

- *Stanford University*, Donald Knuth
  - **Classical Tests**
- *Florida State University*, George Marsaglia
  - **DIEHARD**
- *Queensland University of Technology*, Helen Gustafson, Edward Dawson, William Caelli and Lauren Nielsen
  - **Crypt-X**
- *University of Montreal*, Pierre L'Ecuyer
  - **TestU01 (?)**

Project Goals

- The development of a computer package suitable in the assessment of binary stream randomness.
- Applicable to binary streams produced by both hardware and software based PRNGs.
- Warning:
  - No set of statistical tests can certify a generator as appropriate for usage in a particular application.
  - Statistical testing cannot serve as a substitute for cryptanalysis.

Research Team

- **The NIST RNG TWG**
  - **Computer Security Division**
    - Miles Smid, James Nechvatal, James Dray, San Vo, Juan Soto
  - **Statistical Engineering Division**
    - Andrew Rukhin, David Banks, Stefan Leigh, Mark Vangel, Mark Levenson

NIST Test Suite Strengths

- Diverse research team.
- Full scientific documentation provided (each algorithm based on rigorous math).
- More advanced statistical tests.
- Uniform reporting standard (p-value).

Pseudorandom Number Generators

- ANSI X9.17 PRNG (ANSI X9.17)
- FIPS 186 One Way Function Using DES (G-DES)
- FIPS 186 One Way Function Using SHA-1 (G-SHA)
- ***Blum-Blum-Shub (BBS)***
- ***Micali-Schnorr (MS)***
- **Polynomial Congruential (LCG,QCG,CCG)**
- **Modular Exponentiation (MODEXP)**
- **Exclusive OR (XOR)**

NIST Statistical Test Suite

- Frequency
- Block Frequency
- Cusum
- Runs
- Longest Run Of Ones
- Marsaglia’s Rank*
- Spectral (DFT)
- Template Matchings
- Maurer’s Universal*
- Approximate Entropy
- Random Excursions
- Moving Averages
- Lempel Ziv Complexity
- Linear Complexity*

Evaluation Approaches

- **Analytical**
  - Probability Theory
  - Information Theory
  - Complexity Theory
- **Graphical**
  - Approximate Entropy
  - Spectral Graph
  - Cycle Structure

Evaluation Procedure

- **Null Hypothesis.**
  - Binary stream is random.
- **Compute the test statistic.**
  - Testing is carried out at the bit level.
- **Compute its P-value.**
  - Probability of observing a test statistic at least as extreme as the value actually observed.
- **Compare the P-value to α.**
  - **Success** whenever P-value $\geq \alpha$. **Failure** otherwise.
  - α is chosen *conservatively* in (0.001, 0.01].

Numerical Experiments

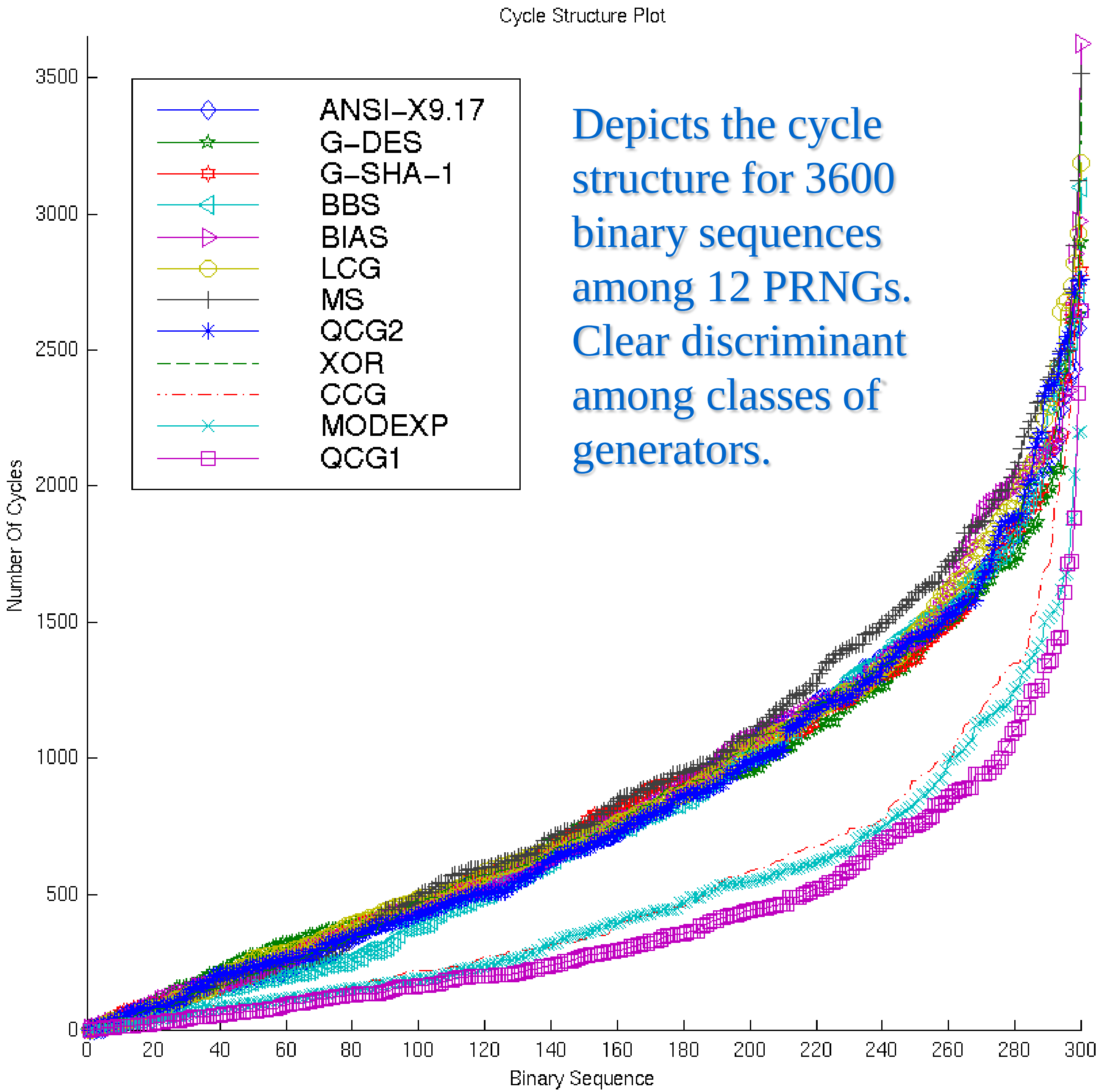
- **Experiment Parameters**
  - 1,000,000 bits/sequence.
  - 300 binary sequences/generator.
- **PRNGs for which:**
  - flaws were not detected
    - ANSI X9.17, G-DES, G-SHA, BBS, MS, LCG, QCG2
  - flaws were detected
    - QCG1, CCG, XOR, MODEXP
    - Statistically significant results detected at the 0.01 level.

Pass Rates at 1% Significance Level

Statistical Test	G-SHA-1	G-DES	X9.17	BBS	MS	QCG II
Frequency	99.67%	99.00%	100.00%	99.00%	99.33%	99.00%
Block Frequency	99.33%	99.33%	98.67%	100.00%	99.00%	97.67%
Cusum Forward	99.00%	98.00%	97.67%	97.67%	98.00%	98.00%
Cusum Reverse	99.33%	97.67%	98.33%	98.33%	98.00%	98.33%
Runs	98.67%	98.33%	99.67%	99.33%	99.33%	99.67%
Longest Run Of Ones	98.67%	99.67%	99.67%	99.33%	99.67%	99.33%
Marsaglia's Rank	98.67%	98.67%	97.67%	100.00%	97.00%	99.33%
Spectral (DFT)	99.67%	99.33%	99.67%	99.33%	99.33%	100.00%
Nonoverlapping Template	99.00%	99.33%	99.00%	98.33%	99.00%	99.33%
Overlapping Template	98.33%	99.33%	98.00%	99.00%	99.67%	99.00%
Maurer's Universal	98.67%	98.67%	98.67%	99.00%	98.00%	99.00%
Approximate Entropy	99.00%	98.33%	99.33%	98.67%	100.00%	99.00%
Random Excursions	99.48%	97.37%	99.48%	100.00%	97.50%	98.91%
Lempel-Ziv Complexity	99.33%	99.67%	99.67%	99.33%	98.33%	99.67%
Linear Complexity	98.67%	98.33%	99.33%	98.67%	99.00%	99.00%

Pass Rates at 1% Significance Level

Statistical Test	XOR	CCG	MODEXP	QCG I	LCG	BIAS
Frequency	99.33%	71.33%	65.00%	58.67%	98.33%	99.33%
Block Frequency	90.33%	100.00%	99.33%	99.33%	98.67%	100.00%
Cusum Forward	97.67%	62.67%	58.33%	51.67%	97.67%	98.00%
Cusum Reverse	99.33%	64.00%	59.00%	51.00%	97.33%	98.33%
Runs	99.33%	0.00%	99.33%	97.67%	98.33%	98.67%
Longest Run Of Ones	99.67%	99.00%	99.67%	100.00%	98.67%	99.67%
Marsaglia's Rank	86.33%	98.33%	98.67%	98.67%	99.67%	98.67%
Spectral (DFT)	100.00%	83.00%	100.00%	100.00%	99.33%	0.00%
Nonoverlapping Template	83.67%	100.00%	98.00%	98.33%	99.00%	99.00%
Overlapping Template	94.67%	99.67%	99.00%	99.67%	98.67%	99.00%
Maurer's Universal	68.33%	99.00%	99.00%	98.67%	98.67%	95.00%
Approximate Entropy	87.67%	0.00%	95.00%	94.33%	99.67%	99.33%
Random Excursions	98.97%	99.12%	98.26%	100.00%	98.98%	98.95%
Lempel-Ziv Complexity	99.00%	98.67%	98.67%	99.33%	99.67%	98.33%
Linear Complexity	0.00%	98.33%	99.67%	99.00%	98.00%	99.67%



Depicts the cycle structure for 3600 binary sequences among 12 PRNGs. Clear discriminant among classes of generators.

Status

- Spring 1998:
  - Release documentation & reference implementation for peer review.
- Summer 1999:
  - Release the statistical test suite and associated documents to the public.

FOR MORE INFO...

http://www.nist.gov/div893/staff/soto/sts.html

Closing Remarks

- Benefits Of Statistical Testing
  – Helps to distinguish between bad PRNGs and good PRNGs.
  – Helps to ensure that the implementation of good PRNGs is in fact producing random looking binary sequences.
  – Helps to evaluate other cryptographic primitives, such as encryption algorithms.

References

- *"A computer package for measuring strength of encryption algorithms,"* H. Gustafson, E. Dawson, L. Nielsen, and W. Caelli, Computers & Security, 13 (1994), pages 687-697.
- *Handbook of Applied Cryptography*, A. Menezes, P. van Oorschot, S. Vanstone, 1997.
- *The Art of Computer Programming, Seminumerical Algorithms, Vol. 2*, Third Edition, D. Knuth, 1998.