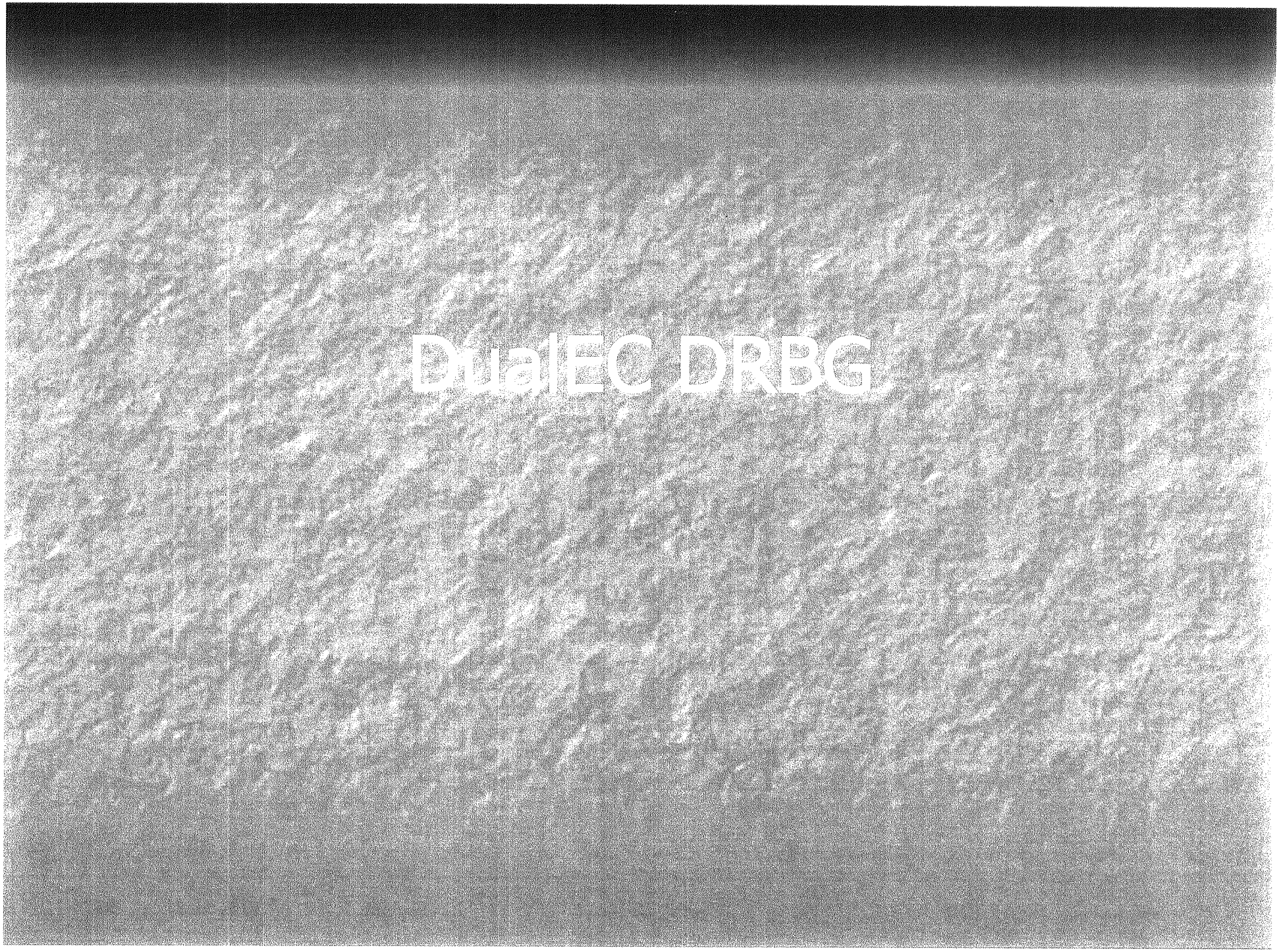
Changes to the RNG web page (http://csrc.nist.gov/CryptoToolkit/tkrng.html):

1. Remove the current Announcement, including the bulleted list.

2. In the new box we discussed, include the following links:
   Agenda
   RNG Development History
   RNG Standard Strategy (coming) [This will need to be added later]
   X9.82, Part 1
   X9.82, Part 3
   Hash and block cipher-based DRBGs
   Number theoretic DRBGs
   X9.82, Part 2 (coming) [This will need to be added later]
   Entropy Sources
   Testing Issues with OS-based Entropy Sources
   Validation Testing and NIST Statistical Test Suite
   Block cipher-based DRBGs (coming) [This will need to be added later]

3. Insert a note that the draft of X9.82 is no longer available for posting to the web site. Also, that comments may be sent to ebarker@nist.gov or John.Kelsey@nist.gov.

4. You have text about future plans further down the page that you may want to change.


DualEC DRBG

Where we are and how we got here...

- Original goals of X9.82 DRBGs:
  - Protecting Internal state
  - Good Randomness properties

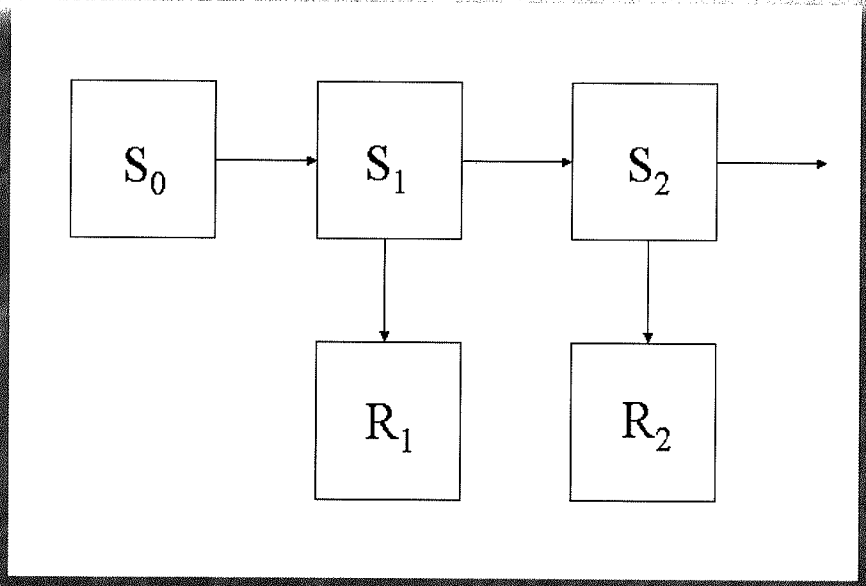
Protection of the internal state is directly tied to the EC discrete log

- Backtracking Resistance
- Outputs

Where we are and how we got here.

$S_i = \varphi(X(S_{i-1} * P))$

$R_i = \varphi(X(S_i * Q))$



Where we are and how we got here.

- Later, Indistinguishability From Random was made a formal requirement.

- This requirement is not directly met by the hardness of the EC Discrete Log problem.

Soul Searching

- NSA had previously done background work on Dual EC DRBG.
- When objections arose we went back, studied the previous work, supplemented it with some new results and began the painful process of Pre-Publication Review.

Simple Observations

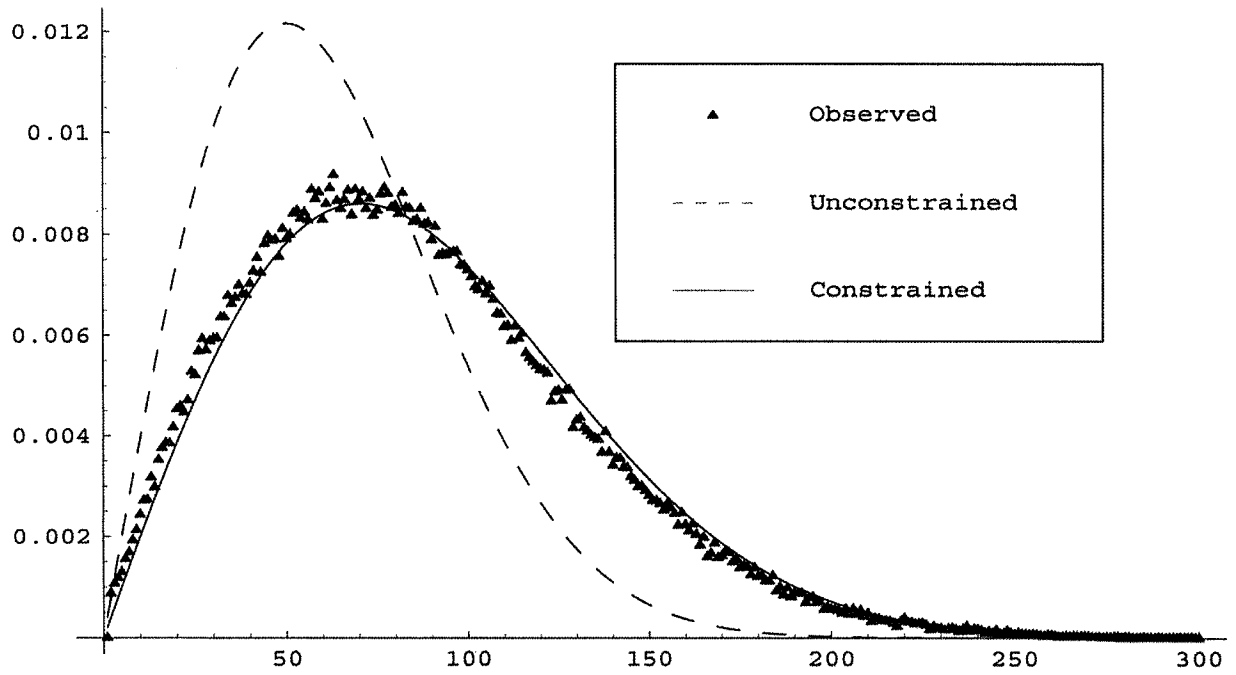
- The internal state values can be viewed as outputs of an iterated function.
- This function has constrained pre-image structure.
  - Each value has at most 3 pre-images.
  - $aP = (x,y)$, then $-aP=(x,-y)$ and $(n+a)P = (x,y)$
    - (3^{rd} case relevant only when a is very small)

This is true independent of the size of the curve.

Results

- Dual EC is expected to have cycle structure which is very much like the output of an iterated random function.
- Simple analysis of the truncation bias shows that it is less than the x-coordinate bias.
- We can quantify the distribution of x-coordinates more precisely.
- We've done some further computational experiments to search for bias in the output.

Distribution of Rho Lengths



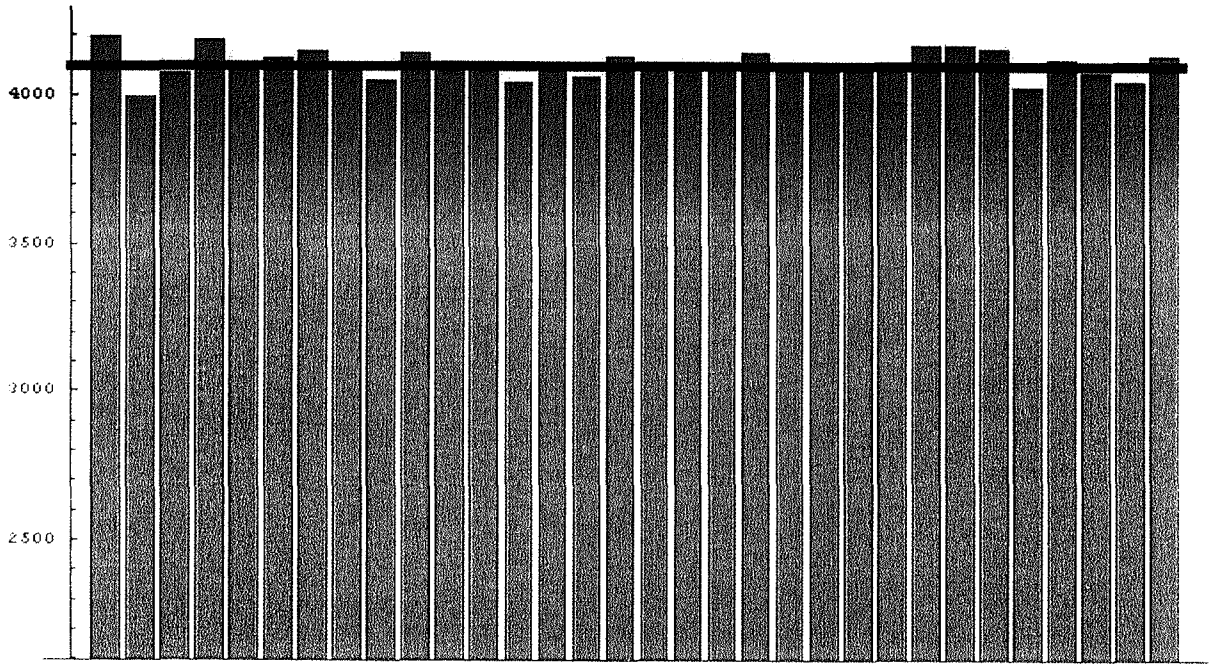
Distribution of X-Coordinates

- For any interval in [0,p-1], the difference in the proportion of distinct x-coordinates in that interval, and the proportion expected to be in that interval if they were distributed uniformly is bounded by

$$K \log^2(p)/\sqrt{p}$$

(when p is sufficiently large)

Distribution of X-Coordinates



Proposed Changes to X9.82 Part 3

- Provide a means for generating P and Q in a verifiable fashion.
- Elimination of the Binary Curves from the DualEC.
- Clarifying text to describe what assurances the EC discrete log problem provides in this setting (and what assurances it is not meant to provide).