RLC FEC Scheme update after IESG review

vincent.roca@inria.fr
TSVWG Nov. 5th, 2018, IETF 103, Bangkok
(Great) comments during IESG review

- most of them for the C code specification of TinyMT32 PRNG
  - distinguish:
    - the **core part** that produces a uint32 PR number number in \([0; 2^{32}-1]\)
      - original TinyMT32 code from M. Saito / M. Matsumoto
    - the **mapping** of the uint32 PR number to a smaller \([0; \text{maxv}-1]\) range
      - our own code (missing in TinyMT32)
    - this mapping must not introduce undesired biases, nor be too computing intensive!
(Great) comments during IESG review (2)

- **concern 1**: is it safe across all possible platforms (CPU/OS/compiler/future version of C)?
  - deterministic PRNG behavior is a MUST
  - proposal: tests under progress (Emmanuel Baccelli) across Corte M* tiny devices, running RIOT OS, in addition to traditional platforms
    - core PRNG: \(\Rightarrow\) seems okay
    - mapping to a smaller range: \(\Rightarrow\) to be done
  - we cannot warrant it will continue to work with any future CPU/C flavor/compiler/…
    - … yet it’s a 113 line source code, comments included
(Great) comments during IESG review (3)

- **concern 2:** is the BSD-like license compatible with “IETF RFC license”?
  - no way to avoid the problem: the C code is the PRNG specification (it’s a complex PRNG)
  - TinyMT32 follows a BSD style license… should facilitate integration, we can also discuss with authors

- **concern 3:** are we using the PRNG the right way during mapping?
  - probably not, we we using floating point calculations (deterministic?)
  - proposal: switched to full integer solutions
Next steps

• address other comments on RLC and FECFRAME (easier)
• work to be done on PRNG to address concerns 1 and 2
  ▪ on progress (authors)

• clarification needed for concern 2 (licensing)
  ▪ on progress discussions with IESG
  ▪ ask TinyMT32 authors?

• Question: does it make sense to extract the PRNG an put it in a separate document?
  ▪ normative reference from FEC Scheme to this TinyMT32 document
  ▪ increased visibility and easier reuse of PRNG in a different context